Parallels Mac Management for Microsoft SCCM 2012

Administrator's Guide

v3.1

Copyright © 1999-2014 Parallels IP Holdings GmbH and its affiliates. All rights reserved.

Parallels IP Holdings GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 632 0411
Fax: + 41 52 672 2010
www.parallels.com
Copyright © 1999-2014 Parallels IP Holdings GmbH and its affiliates. All rights reserved.
This product is protected by United States and international copyright laws. The product's underlying technology, patents, and trademarks are listed at http://www.parallels.com/trademarks.
Microsoft, Windows, Windows Server, Windows NT, Windows Vista, and MS-DOS are registered trademarks of Microsoft Corporation.
Apple, Mac, the Mac logo, Mac OS, iPad, iPhone, iPod touch, FaceTime HD camera and iSight are trademarks of Apple Inc., registered in the US and other countries.
Linux is a registered trademark of Linus Torvalds.
All other marks and names mentioned herein may be trademarks of their respective owners.

Contents

Introduction 7

About This Guide 7

About Parallels Mac Management for Microsoft SCCM 2012 7

Deploying Parallels Mac Management for Microsoft SCCM 2012 9

Parallels Mac Management Component Overview 9

Checking Installation Requirements 10

Checking User Rights Requirements 14

User Rights Required for Installing and Configuring Parallels Mac Management 14

User Rights Required for Running Parallels Configuration Manager Proxy Service 18

Configuring Certificate Authorities and PKI Integration 20

Certificate Authority and PKI Integration Overview 20

Deploying PKI Certificates 21

Creating Certificate Templates for Parallels Proxy and Macs 28

Creating Special Security Group 30

Installing Parallels Mac Management for Microsoft SCCM 2012 31

Parallels Mac Management for Microsoft SCCM Setup Wizard 31

Parallels Configuration Manager Proxy Configuration Wizard 32

Parallels NetBoot Server Configuration Wizard 34

Upgrading Parallels Mac Management for Microsoft SCCM 2012 36

Configuring Configuration Manager Boundaries 36
Configuring Windows Firewall 37
Viewing Proxy Service Certificate Details 37
Migrating Configuration Manager Proxy 38
Deploying Parallels Mac Client 41
Deploying Mac Client via Network Discovery 41
Installing Mac Client Using Interactive Installer 44
Installing Mac Client Using Installation Script 46
Configuring Mac OS X Firewall 47
Verifying Mac Client Deployment 48
Updating Parallels Configuration Manager Proxy Connection URL 48
Upgrading Parallels Mac Client 49
Uninstalling Parallels Mac Client 49
Managing Parallels Mac Client 51
Viewing Parallels Mac Client Properties 51
Initiating Policy Retrieval 53
Sending Problem Reports From Mac Client 55
Parallels Mac Management Features 57
Using Configuration Manager 2012 Console 57
Understanding Collections in Parallels Mac Management 57
Hardware and Software Inventory 58
Configuring Inventory Settings 58
Viewing Inventory Data 59
Desired Configuration Management 59
Deploying OS X Configuration Profile 59
Enforcing FileVault 2 Encryption 66
Enforcing Parallels Desktop Preferences 79
Enforcing Parallels Desktop VM Settings 81
Using Scripts to Assess Compliance 82
Deploying Configuration Baseline 86
Receiving DCM Reports 87
Application Management 88
Choosing Installation Type 88

Preparing Mac Application for Configuration Manager 89
Creating Configuration Manager Application 90
Configuring Deployment Type 91
Deploying Mac Application 93
Installing Application on a Mac 95
Using Parallels Application Portal 96
Software Distribution 97
Creating Software Distribution Package 97
Sending Package to Distribution Point 100
Deploying Software 100
Viewing Status of a Package 101
Deploying Mac OS X Images 101
Deploying Parallels Desktop and Virtual Machines on Macs 105
Deploying SCCM Client in Windows Running in a Virtual Machine 107
Providing Remote Assistance to Mac Users 109
Problem Reporting and Monitoring 111
Sending Problem Reports Using Configuration Manager Console 111
Sending Problem Reports Using Windows Reporting Utility 112
Sending Problem Reports from Mac Client 113
Using Problem Monitoring Utility 113
Tracking Apple Warranty Status of Macs 116
Technical Reference 118
Wizard Pages 118
Parallels Configuration Manager Proxy Configuration Wizard 118
Parallels NetBoot Server Configuration Wizard 124
Software Distribution Wizards 128
Property Pages 129
Parallels Discovery Properties 129
Dialog Pages 134
Desired Configuration Management Dialogs 134
New Subnet Assignment Dialog 142
Custom Schedule Dialog 143
Max OS X User Account Dialog 144
Problem Report for Parallels Mac Management for Microsoft SCCM Dialog 144

Send Problem Report Dialog 145
Problem Reports Dialog 145
Appendices 147
Ports Used by Parallels Mac Management 147
Log Files in Parallels Mac Management for Microsoft SCCM 148
Changing Log File Rotation Limits 151
Parallels Mac Management Database 153
Index 154

CHAPTER 1

Introduction

In This Chapter

About This Guide 7
About Parallels Mac Management for Microsoft SCCM 2012 7

About This Guide

This guide contains information about how to deploy and use Parallels Mac Management for Microsoft SCCM 2012. The guide is intended for IT administrators.

About Parallels Mac Management for Microsoft SCCM 2012

Parallels Mac Management for Microsoft SCCM 2012 is a software product that extends Microsoft System Center Configuration Manager 2012 and 2012 R2 with support for Mac OS X systems. With Parallels Mac Management you can manage Mac and Windows computers using Configuration Manager as your only management system.

Parallels Mac Management adds the following Mac management features to SCCM 2012 and SCCM 2012 R2:

Feature	Description
Network discovery of Mac computers (p. 41)	Network discovery allows to automatically find Mac computers on a network and assign them to a Configuration Manager site.
Inventory of Mac hardware and installed applications (p. 58)	Mac hardware and software inventory is automatically collected and can be viewed in the Configuration Manager console.
Mac OS X image deployment (p. 101)	Allows to automate the deployment of OS X on managed Mac computers.
Mac OS X software and patch distribution (p. 97)	Allows to use the standard Configuration Manager Software Distribution functionality to install software and updates on managed Macs.
Parallels Application Portal (p. 88)	Allows Mac users to view and install OS X applications made available to the user by their

	system administrator.
Mac OS X configuration management via Configuration Profiles (p. 59)	Allows to configure Macs and enforce compliance with SCCM Desired Configuration Management functionality.
FileVault 2 Encryption Management (p. 66)	Allows to use FileVault 2 to encrypt the contents of disk drives on managed Macs with the ability to set an institutional or a private recovery key.
Parallels Desktop and Parallels virtual machine configuration management (p. 79)	Allows to configure Parallels Desktop and Parallels virtual machines installed on a Mac.

Parallels Mac Management fully integrates with the Configuration Manager console, so IT administrators can manage Mac and Windows computers using the same familiar graphical user interface.

CHAPTER 2

Deploying Parallels Mac Management for Microsoft SCCM 2012

This chapter contains information about how to deploy Parallels Mac Management for Microsoft SCCM 2012 in an enterprise computing environment.

In This Chapter

Parallels Mac Management Component Overview 9
Checking Installation Requirements 10
Checking User Rights Requirements 14
Configuring Certificate Authorities and PKI Integration 20
Installing Parallels Mac Management for Microsoft SCCM 2012 31
Configuring Configuration Manager Boundaries 36
Configuring Windows Firewall 37
Viewing Proxy Service Certificate Details 37
Migrating Configuration Manager Proxy 38

Parallels Mac Management Component Overview

Parallels Mac Management consists of the following components:

- **Parallels Configuration Manager Proxy**. This is a Windows service application that acts as a proxy between SCCM and Mac computers. The application must be installed on a computer running Windows Server 2008 SP2 or later.
- **Configuration Manager Console Extension**. This component consists of a set of dynamic libraries that extend the Configuration Manager console to provide a graphical user interface enabling you to manage Mac OS X computers. The component must be installed on the computer where the Configuration Manager console is running.
- **NetBoot Server**. NetBoot is a technology from Apple that enables Mac computers to boot from a network. You need to install this component if you plan to deploy Mac OS X images on Mac computers. The component must be installed on a computer running Windows Server 2008 SP2 or later.
- **Parallels Mac Client**. This is a client software that enables communication between the Mac computer on which it is installed and the Parallels Configuration Manager Proxy.

Supported SCCM Versions

Parallels Mac Management supports Microsoft System Center Configuration Manager 2012 and 2012 R2. Please make sure that you have the latest service pack and critical updates installed.

Supported Windows Versions

Parallels Mac Management supports all versions of Windows that are supported by System Center Configuration Manager 2012 and 2012 R2.

Supported OS X Versions

The following versions of OS X operating system are supported:

- OS X 10.6 Snow Leopard
- OS X 10.7 Lion
- OS X 10.8 Mountain Lion
- OS X 10.9 Mavericks
- OS X 10.10 Yosemite

Checking Installation Requirements

Before you install Parallels Mac Management for Microsoft SCCM 2012, use the instructions provided here to ensure that the installation requirements are met.

Windows computers requirements

Parallels Configuration Manager Proxy and NetBoot Server must be installed on a computer(s) running Windows Server 2008 SP2 or later. This can be a dedicated server (or two separate dedicated servers for each component) or a server running Microsoft System Center Configuration Manager. The Configuration Manager Console Extension component must be installed on a Windows computer running the Configuration Manager console.

Check the Parallels Configuration Manager Proxy requirements

The computer on which Parallels Configuration Manager Proxy will be installed must have the .NET Framework 4.0 installed.

Check the NetBoot Server requirements

The computer on which the NetBoot Server will be installed must meet the following requirements:

- The Distribution Point role is installed on this server.
- The server is a PXE service point.
- WDS is installed and running. If WDS and DHCP are both installed on this server, the **Do not listen on port 67** option must be selected in the WDS service properties.
- BITS 4.0 is installed.
- Verify that the user configuring the NetBoot Server has sufficient privileges. See the following KB article: http://kb.parallels.com/117937

Verify that the Management Point role is installed

To do so, enter the following URL into a Web browser (substitute `http` with `https` if that's what your Management Point is using):

```
http://[MPNAME]/sms_mp/.sms_aut?mplist
```

where `[MPNAME]` is a fully qualified domain name of the Management Point server.

The URL should open an XML file without an error.

Verify that the Distribution Point role is configured properly

In the Configuration Manager console:

1. Navigate to **Administration** / **Site Configuration** / **Servers and Site System Roles**.
2. Select your site in the right pane.
3. In the **Site System Roles** pane, right-click the **Distribution Point** role and then click **Properties** in the context menu.
4. In the **Distribution Point Properties** dialog do the following:
   - On the **General** tab page, select **HTTP** or **HTTPS** in the **Specify how client computers communicate with this distribution point** group. If you'll be using Public Key Infrastructure (PKI) for authentication, you need to select **HTTPS**. The PKI integration is described in detail in **Configuring Certificate Authorities and PKI Integration** section (p. 20).
   - If you've selected **HTTP**, check the **Allow clients to connect anonymously** option.

Check the Internet Information Services (IIS) settings on the Distribution Point server

In Windows Server 2008:

1. Click **Start** > **Administrative tools** > **Internet Information Services (IIS) Manager**.
2. Open **Default Web Site** and double-click **Authentication** in IIS.
3. Check that **Windows Authentication** is enabled.
4. Open **Default Web Site** and double-click **Authorization Rules** in IIS.

5 Check that authorization is allowed to all users

Verify that WebDAV is enabled

In Windows Server 2008:

1 Click **Start** > **Administrative tools** > **Internet Information Services (IIS) Manager**.

2 Select the server name and expand **Sites**.

3 Click **Default Web Site**.

4 Double-click **IIS** > **WebDAV Authoring Rules**.

If WebDAV is enabled, the **Enable WebDAV** action should not be available in the **Actions** pane. The central pane should contain the Authoring Rule with the **All content**, **All users** and **Read** options selected.

5 Select the role and click **WebDAV Settings** in the **Actions** pane.

6 In the **WebDAV Settings** workspace (under **Property Behavior**) make the following changes:

- Set the **Allow anonymous property queries** option to **True**.
- Set **Allow Custom Properties** to **False**.
- Set **Allow property queries with infinite depth** to **True**.
- If this is a BITS-enabled Distribution Point, then under **WebDAV Behavior**, set **Allow hidden files to be listed** to True.

Verify that Configuration Manager Boundaries are configured properly

In the Configuration Manager console:

1 Check the boundary settings at the following location: **Administration** / **Hierarchy Configuration** / **Boundaries**.

2 In addition, **Boundary Groups** must also be configured in SCCM 2012.

For details, see **Configuring Configuration Manager Boundaries** (p. 36).

Check that the Reporting Point role is installed

Note: The Reporting Point role is not required for Parallels Mac Management installation, but it is needed for the reporting functions to work.

1 In the Configuration Manager console:

2 Navigate to **Administration** / **Site Configuration** / **Servers and Site System Roles**.

3 Verify that the Reporting services point role exists.

4 Navigate to **Monitoring** / **Reporting** / **Reports**.

5 Right-click any of the available reports and check that the **Run** item is available in the pop-up menu.

Check that the Report Viewer is installed

Note: The Report Viewer is not required for Parallels Mac Management installation, but it is needed for viewing reports.

On the computer running the Configuration Manager console:

1 Click **Start** > **Control Panel** > **Programs and Features**.

2 Verify that **Microsoft Report Viewer Redistributable** is installed.

Check that the firewall is configured properly in Windows and OS X

Please see the complete instructions in the **Configuring Windows Firewall** (p. 37) and **Configuring Mac OS X Firewall** (p. 47) sections.

Verify that your network environment is configured properly

See the following KB article: http://kb.parallels.com/118518

Verify that your Mac computers have network access to SCCM site servers and computers on which you'll install Parallels Mac Management

Use the `traceroute` command in Mac OS X and `tracert` in Windows to verify network access.

Access to the following servers needs to be checked:

- A server that will be running Parallels Configuration Manager Proxy.
- The Active Directory server.
- The Management Point role server.
- The Distribution Point role server.

Check the IP address of the DNS server in OS X network preferences on a Mac:

1 In Mac OS X, open **System Preferences** / **Network.**

2 Click the **Advanced** button, click the **DNS** tab and see the DNS Servers section. Add the DNS server address if it's missing.

Check the date and time synchronization

Date and time must be synchronized between the servers running the Configuration Manager, Configuration Manager Proxy, Active Directory, Management Point, Distribution Point, and the Mac computers. If that's not done, the Parallels Mac Client registration and the Mac management operations (specifically, policy downloading and updating) may not work correctly.

Review the ports used by Parallels Mac Management

The ports used by Parallels Mac Management should not be used by other programs. For the list of ports see **Ports Used by Parallels Mac Management** (p. 147).

Checking User Rights Requirements

To install and configure Parallels Mac Management for SCMM the user performing the installation must have sufficient rights. To run the Parallels Configuration Manager Proxy service, its user account must also have sufficient rights. The following topics describe the required user rights and provide detailed information on how to verify and to set them.

User Rights Required for Installing and Configuring Parallels Mac Management

To install and configure Parallels Mac Management components on Windows computers, the user performing the installation and configuration must have specific rights. The following provides a summary of the requirements and then describes in detail how to verify and to set the necessary user rights.

Required User Rights Summary

The user installing and configuring Parallels Mac Management must be a domain user with the following rights:

- Permissions to write to the SMS Provider (full write WMI permissions).
- Permissions to use DCOM objects on a server where the SMS Provider is installed (the user must be a member of the Distributed COM Users group).
- Administrative rights in Configuration Manager.
- Permissions to make the following changes in Active Directory:
  - Create the "CN=ProgramData,CN=Parallels,CN=Parallels Management Suite" container, or (if the container already exists) create child objects in it.
  - Create the "CN=ParallelsServices" container, or (if the container already exists) make changes to its contents.

- Permissions to register and unregister Service Principal Names for the user account used to run the Parallels Configuration Manager Proxy service.
- Administrative rights on the computer where the installation is performed.

The following step-by-step instructions describe how to create a Windows user with the rights outlined above.

Create a new domain user

Note: You may skip this section if you want to use an existing domain user.

1. On the computer running Active Directory, click **Start** > Administrative **Tools** > **Server Manage**r.
2. In the **Server Manager** window, navigate to **Roles** / **Active Directory Domain Services** / **Active Directory Users and Computers** / *<domain-name>*.
3. Right-click **Users** and select **New** > **User** in the context menu.
4. In the **New Object – User** dialog, type **Full name**, **User logon name**, and click **Next**.
5. Type and confirm the password in the **Password** and **Confirm password** fields.
6. Click **Next**. Click **Finish**.

Add the user to the Distributed COM Users group

The user must be a member of the group to work with the SMS Provider through WMI. This is needed when Parallels Configuration Manager Proxy and the SMS Provider are installed on different computers.

1. In the **Server Manager** window, right-click the domain user that you created and select **Add to a group…** in the context menu.
2. Add the user to the **Distributed COM Users** group.

Grant the user permissions to write to WMI

Parallels Configuration Manager Proxy needs rights to alter the SMS WMI workspace by adding new classes.

1. In the **Server Manager** window, navigate to **Configuration** / **WMI Control**.
2. Right-click **WMI Control** and select **Properties** in the context menu.
3. Select the **Security** tab in the **WMI Control Properties** dialog.
4. In the **Namespace** navigation tree, select **Root** / **SMS** / **site_***<site-code>* and then click the **Security** button.
5. Click the **Add** button, find your user, and click **OK**. The user will appear in the **Group or user names** list.

6 Grant the user **Full Write** permissions.

7 Click **OK** to close the dialog.

8 Click **OK** to close the **WMI Control Properties** dialog.

Grant the user administrative rights on the computer(s) where you'll be installing Parallels Configuration Manager Proxy and NetBoot Server

1 Log in to a computer where you'll be performing the installation of a given component.

2 Open **Server Manager** and navigate to **Configuration** / **Local Users and Groups** / **Groups**.

3 Right-click the **Administrators** group and select **Properties** in the context menu.

4 In the **Select Users** dialog, click the **Add** button and add the domain user you've created earlier.

5 Click **OK** and then click **OK** again.

On a computer that will be running the NetBoot Server, the user must also have local and remote read access to SMS Provider. For the complete information, please read **kb.parallels.com/117937** (**http://kb.parallels.com/117937**).

Grant the user administrative rights in Configuration Manager

1 Log in to the computer running the Configuration Manager console and open the console.

2 Navigate to **Administration** / **Overview** / **Security**.

3 Right-click **Administrative Users** and select **Add User or Group** in the context menu.

4 In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.

5 Click the **Add...** button in the **Assigned security roles** section.

6 In the **Available security roles** list, select **Full Administrator** and click **OK**.

7 Click **OK** in the **Add User or Group** dialog.

Create the "CN=ParallelsServices" container in Active Directory and grant the user permissions to write to it

This container is used to store the connection URL of the Configuration Manager Proxy service. If a Mac client loses the Proxy connection, it can retrieve the connection URL from this container.

Note: Skip steps 1 through 6 if the container already exists.

1 On the computer running Active Directory, click **Start** > **Administrative Tools** > **ADSI Edit**.

2 In the **ADSI Edit** window, navigate to **Default naming context** / **DC=**<*domain*>,**DC=**<*com*> / **CN=System**.

3 Right-click **CN=System** and select **New** > **Object...** in the context menu.

4 In the **Select a class** list, select **container** and click **Next**.

5 In the **value** field, type "ParallelsServices" (without quotes) and click **Next**.

6 Click **Finish**.

7 In the **ADSI Edit** window, right-click **CN=ParallelsServices** and then select **Properties** in the context menu.

8 In the container properties dialog, select the **Security** tab.

9 Add the domain user that you created earlier to the **Group or user names** list and grant the user **Read**, **Write**, and **Create all child objects** permissions.

Create the "CN=Parallels Management Suite" container and grant the user permissions to write to it

This container is used for storing the Parallels Mac Management role-based access control information (RBAC).

Note: Skip steps 1 through 7 if the container already exists.

1 In the **ADSI Edit** window, navigate to **Default naming context** / **DC=**<*domain*>,**DC=**<*com*> / **CN= Program Data**.

2 Right-click **CN= Program Data** and then select **New** > **Object...** in the context menu.

3 In the **Select a class** list, select **container** and click **Next**.

4 In the value field, type "Parallels" (without quotes), click **Next** and then click **Finish**.

5 In the **ADSI Edit** window, right-click **CN= Parallels** and click **New** > **Object...** in the context menu.

6 Select container and click **Next**. Type "Parallels Management Suite" and click **Next**.

7 Click **Finish**.

8 Right-click **CN=Parallels Management Suite** and then click **Properties** in the context menu.

9 Select the **Security** tab and add your domain user to the **Group or user names** list.

10 Grant the user **Read**, **Write**, and **Create all child objects** permissions.

Grant the user permissions to read/write Service Principal Name

These rights are required for the RBAC functionality. The Parallels Configuration Manager Proxy service account must have a registered Service Principle Name (SPN) for Kerberos connections. By default (with some exceptions) users are not permitted to register SPN to their own accounts.

1 In the **ADSI Edit** window, navigate to the **CN=Users** node and select the user that will be used to run the Parallels Configuration Manager Proxy service.

Please note that the user you select in this step must be the user that will be used to run the service, not the user installing it. If you'll be using the same user to install and to run the Parallels Configuration Manager Proxy service, then select the domain user that you created in previous steps.

2 Right-click the user, select **Properties** in the context menu, and then click the **Security** tab in the user properties dialog.

3 Click the **Advanced** button in the **Permissions** section.

4 In the **Advanced Security Settings** dialog, select the user that will be installing and configuring Parallels Mac Management and click the **Edit** button.

5 In the **Permission Entry** dialog, click the **Properties** tab.

6 In the **Apply to** drop-down list, select **This object only**.

7 In the **Permissions** list, select the following permissions:

- **Read servicePrincipalName**
- **Write servicePrincipalName**

8 Click **OK** three times to close all dialogs.

User Rights Required for Running Parallels Configuration Manager Proxy Service

Parallels Configuration Manager Proxy is installed in Windows as a service application. When configuring Parallels Configuration Manager Proxy, you'll be asked to specify a user account for running the service. The user you select must have specific rights. The following provides a summary of the requirements and then describes in detail how to verify and set the necessary user rights.

Required User Rights Summary

The user account under which the Parallels Configuration Manager Proxy runs must be a domain user with the following rights:

- Permissions to write to the SMS Provider (full write WMI permissions).
- Permissions to use DCOM objects on a server where the SMS Provider is installed (the user must be a member of the Distributed COM Users group).
- Administrative rights in Configuration Manager.
- Administrative rights on the computer where the service is running.

The following step-by-step instructions describe how to create a domain user with the rights outlined above.

Create a New Domain User

Note: You may skip this section if you want to use an existing domain user.

1. On the computer running Active Directory, click **Start** > Administrative **Tools** > **Server Manage**r.
2. In the **Server Manager** window, navigate to **Roles** / **Active Directory Domain Services** / **Active Directory Users and Computers** / <*domain-name*>.
3. Right-click **Users** and select **New** > **User** in the context menu.
4. In the **New Object – User** dialog, type **Full name**, **User logon name**, and click **Next**.
5. Type and confirm the password in the **Password** and **Confirm password** fields.
6. Click **Next**. Click **Finish**.

Add the User to the Distributed COM Users Group

1. In the **Server Manager** window, right-click the domain user that you created and select **Add to a group…** in the context menu.
2. Add the user to the **Distributed COM Users** group.

Grant the User Permissions to Write to WMI

1. In the **Server Manager** window, navigate to **Configuration** / **WMI Control**.
2. Right-click **WMI Control** and select **Properties** in the context menu.
3. Select the **Security** tab in the **WMI Control Properties** dialog.
4. In the **Namespace** navigation tree, select **Root** / **SMS** / **site_**<*site-code*> and then click the **Security** button.
5. Click the **Add** button, find your user, and click **OK**. The user will appear in the **Group or user names** list.
6. Grant the user **Full Write** permissions.
7. Click **OK** to close the dialog.
8. Click **OK** to close the **WMI Control Properties** dialog.

Grant the User Administrative Rights in Configuration Manager

1. Log in to the computer running the Configuration Manager console and open the console.
2. Navigate to **Administration** / **Overview** / **Security**.
3. Right-click **Administrative Users** and select **Add User or Group** in the context menu.
4. In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.

5 Click the **Add...** button in the **Assigned security roles** section.

6 In the **Available security roles** list, select **Full Administrator** and click **OK**.

7 Click **OK** in the **Add User or Group** dialog.

Grant the User Administrative Rights on the Local Computer

1 Log in to the computer where you'll be installing Parallels Configuration Manager Proxy.

2 Open **Server Manager** and navigate to **Configuration** / **Local Users and Groups** / **Groups**.

3 Right-click the **Administrators** group and select **Properties** in the context menu.

4 In the **Select Users** dialog, click the **Add** button and add the domain user you've created earlier.

5 Click **OK** and then click **OK** again.

Configuring Certificate Authorities and PKI Integration

Parallels Mac Management can be directly integrated with Certificate Authorities (CA) and Public Key Infrastructure (PKI). Such integration enables the use of certificates for advanced user authentication and secure access to SCCM.

If you would like to integrate Parallels Mac Management with CA and PKI, you need to complete the steps described in the following subsections prior to installing Parallels Mac Management. If you are not planning on using PKI, you can skip this section and continue with **Installing Parallels Mac Management for Microsoft SCCM 2012** (p. 31).

If you are not sure whether you'll be using PKI, you can skip this section and perform the integration later by completing the steps described here and reconfiguring the Parallels Configuration Manager Proxy.

Certificate Authority and PKI Integration Overview

By integrating Parallels Mac Management with Certificate Authority and PKI you'll be able to:

- Obtain security certificates for assigned Macs from a Certificate Authority trusted by SCCM.
- Secure the communication between Mac computers and SCCM by using mutual authentication and encrypted data transfers.

General Requirements

The following versions of SCCM are supported:

- SCCM 2012

- SCCM 2012 SP1
- SCCM 2012 R2

Certificate Authority on the following versions of Windows is supported:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Note: Integration is provided for Microsoft Certificate Services only.

The following subsections describe what needs to be done in order to enable integration of Public Key Infrastructure with Parallels Mac Management. Please note that the steps described here should be performed once for the entire SCCM infrastructure, not for each Parallels Configuration Manager Proxy on each site.

Deploying PKI Certificates

This section describes how to deploy Public Key Infrastructure certificates for use with System Center Configuration Manager 2012.

Installing Active Directory Certificate Services Role

Install and configure the **Active Directory Certificate Services** role as an enterprise root certification authority (CA) on Windows Server 2008 Enterprise Edition:

1. In Windows, click **Start** > **Administrative Tools** > **Server Manager**.
2. In **Server Manager**, right-click **Roles** and then click **Add Roles**. The **Add Roles Wizard** opens.
3. Click **Next** on the **Before You Begin** page.
4. On the **Select Server Roles** page, select the **Active Directory Certificate Services** role and click **Next**.
5. Click **Next** on the **Introduction to Active Directory Certificate Services** page.
6. On the **Select Role Services** page, select **Certification Authority** and click **Next**.
7. On the **Specify Setup Type** page, select **Enterprise** and click **Next**.
8. On the **Specify CA Type** page, select **Root CA** and click **Next**.
9. On the **Set Up Private Key** page, select **Create a new private key** and click **Next**.
10. Skip the **Configure Cryptography for CA**, **Configure CA Name**, **Set Validity Period**, and **Configure Certificate Database** pages.

11 On the **Confirm Installation Selections** page, click **Install** and wait for the role installation to finish.

12 Review the info on the **Installation Results** page and click **Close**.

Deploying Certificate to Web Server

The Web Server certificate must be deployed to site systems that run IIS. This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site system servers that run IIS and that are configured in Configuration Manager to use HTTPS. When used with SCCM 2012 SP1 and SCMS 2012 R2, the certificate may also be required on management points when the client notification traffic falls back to using HTTPS.

To create a certificate template for SCCM site systems and to add this template to CA, follow the instructions provided below.

Create a group containing site system servers that run IIS

To create a group:

1 In Windows, click **Start** > **Administrative Tools** > **Server Manager**.

2 In the **Server Manager** tree, navigate to **Roles** / **Active Directory Domain Services** / **Active Directory Users and Computers** / <*domain-name*> / **Computers**.

3 Right-click **Computers** and then click **New** > **Group**.

4 Type the group name (e.g. ConfigMgr IIS Servers) in both "Group name" fields. Select the Global and the Security options. Click OK.

5 Right-click the group that you just created and click **Properties**.

6 Select the **Members** tab and click **Add**.

7 Add the servers with site systems (with IIS) to the group.

Click **OK** to close the group properties dialog.

Create and issue a Web server template

To create a template:

1 In Windows, click **Start** > **Administrative Tools** > **Certification Authority**.

2 In the **Certification Authority (local)** tree, expand the <*ca-name*> node.

3 Right-click **Certificate Templates** and click **Manage**.

4 In the template list, find the **Web Server** template, right-click it, and click **Duplicate Template** in the context menu.

5 In the Duplicate Template dialog, select the **Windows Server 2003 Enterprise** option (do NOT select Windows Server 2008 Enterprise) and click **OK**.

6 The **Properties of New Template** dialog opens.

7 On the **General** tab page, type the template name (e.g. ConfigMgr Web Server Certificate).

8 Click the **Subject Name** tab and make sure that the **Supply in the request** option is selected.

9 Click the **Security** tab and remove the **Enroll** permissions (i.e. both **Allow** and **Deny** checkboxes are un-selected) for the **Domain Admins** and **Enterprise Admins** groups.

10 While on the **Security** tab page, click the **Add** button and add the **ConfigMgr IIS Servers** group that you created earlier (see above).

11 Grant the **ConfigMgr IIS Servers** group the **Enroll** permission (i.e. the **Allow** checkbox is selected).

12 Click **OK** to close the **Properties of New Template** dialog. Close the **Certificate Templates** console.

13 In the **Certification Authority** window, right-click **Certificate Templates** and click **New** > **Certificate Template to Issue**.

14 In the template list, select the **ConfigMgr Web Server Certificate** template that you just created and click **OK** to enable it.

Specify the Intranet and Internet FQDN values of site system server and install the web server certificate on to the member server that runs IIS

To accomplish this task:

1 Restart the server running the IIS to ensure that it can access the certificate template that you've created in previous steps.

2 Open Microsoft Management Console (run mmc.exe).

3 In the console, click **File** > **Add/Remove Snap-in…**

4 In the **Available snap-ins** list, select **Certificates** and click **Add**.

5 In the dialog that opens select **Computer account** and click **Next**. In the **Select Computer** dialog, make sure that the **Local computer** option is selected and click **Finish**.

6 Click **OK** in the **Add or Remove Snap-ins** dialog.

7 In the certificates console, navigate to **Certificates** / **Personal** / **Certificates**.

8 Right-click **Certificates** and click **All Tasks** > **Request New Certificate** in the context menu. The **Certificate Enrollment** wizard opens.

9 Click **Next** and click **Next** again.

10 On the **Request Certificates** page of the wizard, click **More information is required to enroll for this certificate. Click here to configure settings**.

11 The **Certificate Properties dialog** opens.

12 On the **Subject** tab page, in the **Alternative name** / **Type** field, select **DNS**.

13 In the **Alternative name** / **Value** field, type FQDN values of the site system server (specified in site system properties in Configuration Manager) and click **Add.**

For example:

- If the site system will only accept client connections from the intranet, and the intranet FQDN of the site system server is `server1.internal.contoso.com`, you would enter "server1.internal.contoso.co" in the **Value** field and click **Add**.
- If the site system will accept client connections from both intranet and the Internet, the intranet FQDN of the site system server is `server1.internal.contoso.com`, and the Internet FQDN of the site system server is `server.contoso.com`, you would do the following:

1. Type "server1.internal.contoso.com" in the **Value** field and click **Add**.
2. Type "server.contoso.com" in the **Value** field and then click **Add**.

14 Click **OK** to close the **Certificate Properties** dialog.

15 When back in the **Certificate Enrollment** wizard, select the **ConfigMgr Web Server Certificate** template that you created earlier and click **Enroll**.

16 Wait for the enrollment process to finish and then click **Finish**.

Bind the installed certificate with the IIS Default Web Site on the member server

On the server running the IIS:

1 In Windows, click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2 Navigate to *<computer_name>* / **Sites** / **Default Web Site**.

3 Right-click **Default Web Site** and click **Edit Bindings**.

4 In the **Site Bindings** dialog, select **https** and click the **Edit** button.

5 Select the certificate in the **SSL certificate** drop-down list box. To select the correct certificate, you'll need to use the trial-and-error approach as follows:

1. Select a certificate from the list.
2. Click the **View** button.
3. In the **Certificate** dialog, click the **Details** tab.
4. Scroll to the **Certificate Template Information** field and verify that the certificate is using the **ConfigMgr Web Server Certificate** template that you've created earlier.

6 Once you've selected the correct certificate, click **OK** in the **Edit Site Binding** dialog.

7 Click **Close** in the **Site Bindings** dialog.

Deploying Client Certificate to Distribution Point

Deploying client certificate to a distribution point has two purposes:

- The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages.
- When the **Enable PXE support for clients distribution point** option is selected, the certificate is sent to PXE boot servers so that they can connect to an HTTPS-enabled management point during the deployment of the operating system.

This procedure consists of the following steps:

1. Create and issue a custom workstation authentication certificate template on the Certification Authority computer.
2. Install the custom workstation authentication certificate.
3. Export the client certificate to be used on the distribution point computers.

Creating Custom Workstation Authentication Certificate Template

This section describes how to create a custom certificate template for distribution points that allows the private key to be exported, and adds the certificate template to the certification authority:

On the member server:

1. In Windows, click **Start** > **Administrative Tools** > **Certification Authority**.
2. Expand the **Certificate Templates in Certification Authority (Local)** / *<ca-name>* node.
3. Right-click **Certificate Templates** and click **Manage**.
4. In the template list, find the **Workstation Authentication** template, right-click it, and then click **Duplicate Template** in the context menu.
5. In the **Duplicate Template** dialog, select **Windows Server 2003 Enterprise** (do NOT select Windows Server 2008 Enterprise).
6. The **Properties of New Template** dialog opens.
7. On the **General** tab page, type the template name (e.g. ConfigMgr Client Distribution Point Certificate).
8. Click the **Request Handling** tab and select the **Allow private key to be exported** option.
9. Click the **Security** tab, select the **Enterprise Admins** group and clear the **Enroll** permissions (i.e. both **Allow** and **Deny** options are cleared).
10. Click the **Add** button and then add the **ConfigMgr IIS Servers** group that you created earlier.
11. Select the **ConfigMgr IIS Servers** group and then select **Allow** for the **Enroll** permission.
12. Click **OK**.
13. Close the **Certificate Template Console**.
14. In the certificate snap-in, right-click **Certificate Templates** and click **New** > **Certificate Template to Issue**.
15. In the template list, select the **ConfigMgr Client Distribution Point Certificate** template that you created earlier and click **OK**.

Installing Custom Workstation Authentication Certificate

This section describes how to request and install the custom client certificate on a member server that runs IIS (configured as distribution point):

To accomplish this task:

1. Open Microsoft Management Console (run mmc.exe).
2. Click **File** > **Add/Remove Snap-in…**
3. In the **Available Snap-ins** list, select **Certificates** and lick **Add**.
4. In the dialog that opens, select the **Computer account** option and click **Next**.
5. In the **Select Computer** dialog, make sure that the **Local computer** option is selected and click **Finish**.
6. Click **OK** in the **Add or Remove Snap-ins** dialog.
7. In the certificates console, navigate to **Console Root** / **Certificates (Local Computer)** / **Personal**.
8. Right-click **Certificates** and click **All Tasks** > **Request New Certificate…** in the context menu.
9. The **Certificate Enrollment** wizard opens.
10. Click **Next** on the **Before You Begin** page and click **Next** on the **Select Certificate Enrollment Policy** page.
11. On the **Request Certificates** page, select the **ConfigMgr Client Distribution Point Certificate** template (that's the template that you've created earlier).
12. Click **Enroll** and wait for the enrollment process to finish.
13. Click **Finish**.

Exporting Client Certificate for Distribution Point

This section describes how to export the custom workstation authentication certificate to a file:

To export the certificate to a file:

1. In the certificates snap-in, navigate to **Certificates (Local Computer)** / **Personal** / **Certificates.**
2. In the certificate list, locate the certificate that was issued using the **ConfigMgr Client Distribution Point Certificate** template (look at the **Certificate Template** column value for identification).
3. Right-click the certificate and click **All Tasks** > **Export…** in the context menu. The **Certificate Export Wizard** opens.
4. Click **Next**.
5. On the **Export Private Key** page, click **Yes, export to private key** and click **Next**.

6 Make sure that the **Personal Information Exchange - PKCS #12 (.PFX)** option is selected and click **Next.**

7 On the **Password** page, choose and type the password and click **Next**. You will need to specify the password when you'll be importing the certificate later.

8 On the **File to Export** page, specify the name of the file to export to and click **Next**.

9 Click **Finish**.

10 Store the exported file securely and ensure that it can be accessed from the Configuration Manager console. This certificate is now ready to be imported on a distribution point server.

Switching SCCM Roles from HTTP to HTTPS

If you already have management points and distribution points using HTTP, you need to switch them to use HTTPS as described below.

Management Point

To switch a management point to HTTPS:

1 In the Configuration Manager console, navigate to **Administration** / **Overview** / **Site Configuration** / **Servers and Site System Roles** / *<site-server-name>*.

2 In the **Site System Roles** list, right-click **Management point** and click **Properties** in the context menu.

3 The **Management point Properties** dialog opens.

4 On the **General** page, **Client connections** options, select **HTTPS** and click **OK**.

5 Verify that management point upgrade/reinstallation started and finished successfully and C:\Program Files\Microsoft Configuration Manager\Logs\MPSetup.log contains the records similar to the following:

```
SMSMP Setup Started....
```

…

```
Installation was successful.
~RoleSetup().
```

6 Check the following records in C:\Program Files\Microsoft Configuration Manager\Logs\mpcontrol.log (this log provides the status of MP whether the MP is working as intended or not):

```
SSL is enabled.
```

…

```
Begin validation of Certificate [Thumbprint
4ac41a85e45b805ae765422b18975f356b57de80] issued to
'sccm2012.PRL.LOCAL'
Certificate has "SSL Client Authentication" capability.
```

```
Completed validation of Certificate [Thumbprint
4ac41a85e45b805ae765422b18975f356b57de80] issued to
'sccm2012.PRL.LOCAL'

>>> Selected Certificate [Thumbprint
4ac41a85e45b805ae765422b18975f356b57de80] issued to
'sccm2012.PRL.LOCAL' for HTTPS Client Authentication

Call to HttpSendRequestSync succeeded for port 443 with status code
200, text: OK

…

Successfully performed Management Point availability check against
local computer.
```

Distribution Point

To switch a distribution point to HTTPS:

1. In the Configuration Manager console, navigate to **Administration** > **Overview** > **Site Configuration** > **Servers and Site System Roles** > *<site-server-name>*.
2. In the **Site System Roles** list, right-click **Distribution point** in and click **Properties** in the context menu.
3. The **Distribution point Properties** dialog opens.
4. On the **General** page, select **HTTPS** in **Specify how client computers communicate with this distribution point** section.
5. In the **Create a self-signed certificate or import a PKI client certificate** section, select **Import certificate.**
6. Click the **Browse** button and browse for the exported distribution point certificate.
7. Type the password in the **Password** field (this is the password you specified when you were exporting the certificate).
8. Click **OK** to close the **Distribution point Properties** dialog.

Verifying the Roles

After switching the roles to HTTPS, verify that they are valid. To do so, In the Configuration Manager console, navigate to **Monitoring** / **Overview** / **System Status** / **Site Status** and see the status of the roles. A valid role should have **OK** as the value of the **Status** column.

Creating Certificate Templates for Parallels Proxy and Macs

To enable connection of Macs to HTTPS-enabled SCCM infrastructure the Macs must obtain certificates from the Certificate Authority (CA) trusted by SCCM. PKI certificates secure the communication between the Mac computers and the Configuration Manager site by using mutual authentication and encrypted data transfers.

Creating a Certificate Template for Parallels Configuration Manager Proxy

To create a certificate template:

1. In Windows, click **Start** > **Administrative Tools** > **Certification Authority**.
2. Expand the CA tree, right-click **Certificate Templates** and click **Manage**.
3. The **Certificate Template Console** opens.
4. In the template list, locate **Web Server**, right-click it and then click **Duplicate Template** in the context menu.
5. In the **Duplicate Template** dialog, choose **Windows Server 2003 Enterprise** and click **OK.**
6. The **Properties of New Template** dialog opens.
7. On the **General** page, choose and type the template name (e.g. PMM CM Proxy Certificate).
8. On the **Request Handling** tab page, set **Minimum key size** to 2048 and select the **Allow private key to be exported** option.
9. On the **Properties** tab page, select the **Supply in the request** and the **Use subject information from existing certificates for autoenrollment renewal requests** options.
10. On the **Extension** tab page, add **Client Authentication** to the **Description of Application Policies** list.
11. On the **Security** tab page, add the computer where Parallels Configuration Manager Proxy is installed and the user account under which the Proxy is running. Grant them **Enroll** and **Autoenroll** permissions. Please note that if the Proxy user account is LocalSystem then you only need to add the computer name.
12. Click **OK** to close the **Properties of New Template** dialog.
13. Right click **Certificate Templates** in Certification Authority (Local) → <ca-name> and click New → Certificate Template to Issue in opened context menu
14. Close the **Certificate Template Console**.
15. In the **Certification Authority** window, right-click **Certificate Templates** and click **New** > **Certificate Templates to Issue**.
16. In the **Enable Certificate Templates dialog**, select the **PMM CM Proxy Certificate** template that you've just created and click **OK** to enable it.

Creating a Certificate Template for Mac Computers

To create a certificate template:

1. In Windows, click **Start** > **Administrative Tools** > **Certification Authority**.
2. Expand the CA tree, right-click **Certificate Templates** and click **Manage**.
3. The **Certificate Template Console** opens.

4 In the template list, locate **Workstation Authentication**, right-click it and then click **Duplicate Template** in the context menu.

5 In the **Duplicate Template** dialog, choose **Windows Server 2003 Enterprise** and click **OK.**

6 The **Properties of New Template** dialog opens.

7 On the **General** page, choose and type the template name (e.g. PMM Client Certificate).

8 On the **Request Handling** tab page, set **Minimum key size** to 2048 and select the **Allow private key to be exported** option.

9 On the **Subject Name** tab page, select the **Supply in the request** option. The **Certificate Templates** message box will pop. Click **OK** to close it.

10 On the **Subject Name** tab page, select **Use subject information from existing certificates for autoenrollment renewal requests** option.

11 On the **Extension** tab page, make sure that **Client Authentication** is displayed in the **Description of Application Policies** list. If it's not, add it.

12 On the **Security** tab page, add the computer running Parallels Configuration Manager Proxy and the user account under which the Proxy is running. Grant them **Enroll** and **Autoenroll** permissions. If the Proxy user account is LocalSystem then you only need to add the computer name.

13 Click **OK** to close the **Properties of New Template** dialog.

14 In the **Certification Authority** window, right-click **Certificate Templates** and click **New** > **Certificate Templates to Issue**.

15 In the **Enable Certificate Templates dialog**, select the **PMM Client Certificate** template that you've just created and click **OK** to enable it.

Creating Special Security Group

Create a dedicated security group and grant it the rights to request the certificates from Certification Authority. The following users must be added to this group:

1 An administrator who will be installing and configuring the Parallels Configuration Manager Proxy. This is needed because the Parallels Proxy configuration utility will request the certificate for the Proxy.

2 A user whose account will be used to run the Parallels Configuration Manager Proxy. This is needed because the Proxy will be requesting certificates for Macs.

Installing Parallels Mac Management for Microsoft SCCM 2012

The installation of Parallels Mac Management for Microsoft SCCM 2012 involves installing Parallels Configuration Manager Proxy, Configuration Manager Console Extension, and the optional NetBoot Server. All components are installed using the same installation wizard. If you are installing all of the components on the same computer, you need to run the wizard just once. If you are installing the components on separate computers, run the wizard for each component individually.

Please note that Parallels Configuration Manager Proxy must be installed on each primary SCCM site. If you have secondary sites, you have the following additional Configuration Manager Proxy installation options:

- The Proxy is installed on both the primary and a secondary site. You can use this option to better manage bandwidth utilization between Mac clients, Distribution Point, and Management Point. You must install the Configuration Manager Proxy on the primary site and then on the secondary site (in that order).
- The Proxy is installed on the primary site only. If this option is used, Mac clients will communicate directly with the Configuration Manager Proxy installed on the primary site.

To begin the installation, run the Parallels Mac Management for Microsoft SCCM installation program. This will open the **Parallels Mac Management for Microsoft SCCM Setup** wizard.

Parallels Mac Management for Microsoft SCCM Setup Wizard

To install Parallels Mac Management for Microsoft SCCM, complete each page of the setup wizard as follows:

1. **Welcome**. This is a read-only page that provides a brief overview of the product.
2. **License Agreement**. Contains the legal information. Please read the Parallels End-User License Agreement. If agreed with the terms, select the **I accept the terms in the license agreement** option and click **Next**.
3. **Select Components**. Lists the components that can be installed using the wizard:
   - **Configuration Manager Proxy** — select this option to install the Configuration Manager Proxy component.
   - **Configuration Manager Console Extension** — select this option to install the Configuration Manager Console Extension component.
   - **NetBoot Server** — select this option to install the NetBoot Server component. NetBoot is a technology from Apple that enables Mac computers to boot from a network. You must install this component if you plan to deploy Mac OS X images on Mac computers. The component must be installed on a distribution point server.

If you are installing all of the components on the same server, select all of them. If you are installing them on separate computers, select the component(s) you wish to install.

4 **Ready to Install the Program**. Click the **Install** button to begin the Parallels Mac Management for Microsoft SCCM installation.

5 **Installing Parallels Mac Management for Microsoft SCCM**. Displays the progress bar.

6 **Setup Completed**. Describes whether the installation was successful or not. Depending on which components you've selected to install, the page will contain the following:

- If you've selected to install just the Configuration Manager Console Extension component, the page will contain the **Finish** button which you can click to finish the installation and close the wizard.
- If you've selected to install the Configuration Manager Proxy, the page will contain the **Configure Parallels Mac Management for Microsoft SCCM** option. Make sure the option is selected (it is by default) and click **Finish**. This will close the installation wizard and start the **Parallels Configuration Manager Proxy Configuration Wizard**. You may have to wait a few seconds for the wizard to open. Use the wizard to configure the Configuration Manager Proxy as described below.

Parallels Configuration Manager Proxy Configuration Wizard

To Configure Parallels Configuration Manager Proxy, complete each page of the configuration wizard as follows:

7 **SMS Provider location**. Use this page to specify the hostname or IP address of the server where the SMS Provider is installed. If the SMS Provider and the Configuration Manager Proxy are installed on the same server (the server where you are running this wizard), select the **Local server** option. If the SMS Provider is installed on a different server, select the **Remote server** option and enter the server hostname or IP address.

8 **Configuration Manager Proxy service account**. Use this page to specify the user account that should be used to run the Configuration Manager Proxy service. The account must have read/write access to the SMS Provider. Select the **Local System account** option to use the standard Windows LocalSystem account. Select **This account** to specify a domain account or a local user account. Use the **Password** field to specify the account password. For additional information, see **Prepare Your Computers for Installation**.

9 **Parallels Client certificate management settings**. This page is used to specify which connection type Parallels Configuration Manager Proxy and Mac client will use to communicate with management point and distribution. The page is also used to configure Windows Public Key Infrastructure (PKI) integration with Parallels Mac Management.

> **Note:** In order to configure PKI integration on this page, the PKI must be prepared first. The necessary preparation steps are described in the **Configuring Certificate Authorities and PKI Integration section** (p. 20). If you haven't performed those steps but want to use PKI, you need to prepare the PKI first and then run this wizard again.

Specify the options and values on the page as follows:

- First, select the protocol (HTTP or HTTPS) which the Parallels Proxy and Mac clients will use to communicate with management points and distribution points. To use PKI, select the HTTPS option. If you don't want to use PKI, select the HTTP option. If your distribution points and/or management points are configured to use HTTPS, then the HTTP option will not be available.
- The **Certificate Authority** field is automatically populated with the name of a Certificate Authority detected by the wizard. To specify a different Certificate Authority, click the **Browse** button.
- The **Parallels Proxy certificate template** field is used to specify a certificate template for the Parallels Proxy. Click the **Browse** button to select a template. If the PKI preparation was done properly, you should see the Parallels Proxy certificate template that you created during the preparation stage.
- The **Mac client certificate template** field is used to specify a certificate template for Macs. Click the **Browse** button to select a template. If the PKI preparation was done properly, you should see the Mac template that you created during the preparation stage. Please note that if PKI integration was configured previously on this site and you change the Mac certificate template now, the new Macs will be assigned to the site using the new templates; the previously assigned Macs will continue using the certificates issued with the old template.

If this Parallels Configuration Manager Proxy has already been configured not to use PKI and if there are Macs already assigned to the site, then the Proxy certificate will be re-issued.

10 **Role-based security**. This page allows you to configure the Configuration Manager Proxy role-based access control. The roles are created during the Parallels Mac Management installation and include the following:

- **Administrator**. This role provides access to all of the available Configuration Manager Proxy functions, including Mac registration, Mac management via the Configuration Manager console, problem monitoring functions, and others.
- **Problem Monitor**. This role provides access to the Parallels Mac Management problem monitoring functions. Problem Monitor is a service that monitors the system in real time for possible problems. Members of this role are allowed to use problem monitoring functions, including running the Problem Monitor, viewing reports, deleting reports, and others. See **Using Problem Monitoring Utility** (p. 113) for more info.
- **Enrollers**. This role provides access to the Mac registration functionality. A Mac computer must be registered with the Configuration Manager Proxy before it can be managed via the Configuration Manager console. Members of this role are allowed to run the Mac registration utility on a Mac and register it with the Configuration Manager Proxy. See **Using Mac Client Installation Program and Script (p. 44)** for more info.

- **FileVault Key Administrator**. This role provides read access rights to the Parallels Mac Management SQL Server database (p. 153). The database is installed by Parallels Mac Management on the primary SCCM site and is used to store FileVault 2 recovery information for Mac computers. Users and groups that have read access to the database will be able to retrieve and view the recovery keys for Macs in the Configuration Manager console. By default, only the Domain Admins group is granted access to the database. The Parallels Configuration Manager Proxy account is granted access automatically. To grant access to other users, add them to this role. For more information about managing FileVault 2 encryption on Macs, see **Creating FileVault 2 Configuration Item** (p. 66).

The roles are listed in the **Roles** list. You can select a role and see the default users and groups for it. Depending on your requirements, you can remove a default group and/or add a new group or a user. To remove a group, select it and click the "-" button. To add a group or a user click the "+" button and use the standard **Select Users, Computers, Service Accounts, or Groups** dialog to specify a user or a group.

11 **Configuration Manager Proxy communication ports**. Use this page to specify the TCP ports that the Configuration Manager Proxy will use to communicate with the Configuration Manager Console and the Macs. The Configuration Manager Proxy uses these ports to serve requests from the Configuration Manager console and the Mac clients running on Mac computers. It also publishes its current port configuration in Active Directory and the DNS in order to be discoverable by its clients if the port configuration changes. The default ports should be changed if they are used by some other processes/applications running on the same server as the Configuration Manager Proxy.

12 **Configuration settings summary**. Review the configuration settings on this page. If everything is correct, click **Finish**. The settings will be applied and the Configuration Manager Proxy service will start. A message box will be displayed informing you of the result of the operation.

If you need to reconfigure the Configuration Manager Proxy, you can run the configuration utility later by going to **Start** > **All Programs** > **Parallels** > **Parallels Mac Management for Microsoft SCCM** and clicking the **SCCM Proxy Configuration Utility** item. After you update the configuration, the Configuration Manager Proxy service must be restarted for the changes to take effect.

Note: When the Configuration Manager Proxy service settings are applied, a certificate is deployed for it on the local computer. The Configuration Manager Proxy service account that you specified on the second page of the wizard is granted Read access to the certificate. If you change the account later, you have to make sure that the new account has access to the certificate store and can read the Configuration Manager Proxy certificate private key. For more information, please see View Proxy Service Certificate Details (p. 37).

Parallels NetBoot Server Configuration Wizard

If you've selected the **NetBoot Server** installation option when you installed Parallels Mac Management for Microsoft SCCM, the **Parallels NetBoot Configuration Wizard** will automatically open after you complete the installation.

To configure the Parallels NetBoot server, complete the wizard pages as follows:

1. **SMS Provider location**. Use this page to specify the hostname or IP address of the server where the SMS Provider is installed. If the SMS Provider and the NetBoot server are installed on the same server (the server where you are running this wizard), select the **Local server** option. If the SMS Provider is installed on a different server, select the **Remote server** option and enter the server hostname or IP address.
2. **Parallels NetBoot Server service account**. Use this page to specify the user account that should be used to run the NetBoot service. The account must have read/write access to the SMS Provider. Select the **Local System account** option to use the standard Windows LocalSystem account. Select **This account** to specify a domain account or a local user account. Use the **Password** field to specify the account password. The LocalSystem account is normally used when the SMS Provider is located on the same server as the NetBoot service. A specific account may also be used for the purpose of managing access rights of the NetBoot service. When running on separate computers, the NetBoot service must have DCOM Remote Activation permissions. Permissions on the WMI namespace can be set using **Server Manager > Configuration > WMI Control** snap-in. Permissions for DCOM remote activation can be set via `dcomcnfg.exe` on a computer where the SMS provider is running.
3. **NetBoot images path**. Specify a folder where the NetBoot server will store `.dmg` images.
4. **Support for unknown Macs**. This page allows you to specify whether the NetBoot server is allowed to work with Macs not assigned to the SCCM site. A Mac assigned to the site can be fully managed via SCCM. An unknown Mac is recognized on the network, but has not joined the SCCM site and therefore cannot be managed. You can enable the NetBoot server functionality for unknown Macs, so you can deploy Mac OS X images on them. Select the **Enable unknown Macs support** option to enable this feature. If the option is not selected, the NetBoot server will work only with Macs assigned to the site.
5. **Configuration settings summary**. Review the configuration settings on this page. If everything is correct, click **Finish** to apply the configuration settings. Once the process is complete, the **Configuration progress** window will display the results.

If you need to reconfigure the NetBoot Server, you can run the configuration utility later by going to **Start** > **All Programs** > **Parallels** > **Parallels Mac Management for Microsoft SCCM** and clicking the **NetBoot Server Configuration Utility** item.

Note: Depending on your network topology, you may have to configure UDP traffic forwarding so DHCP broadcast packets from Mac computers can reach the DHCP server and the NetBoot server. For the complete information about setting up the network environment for NetBoot, please read **KB article 118518** (**http://kb.parallels.com/en/118518**). Please also see **Ports Used by Parallels Mac Management** (p. 147) for the list of ports used by NetBoor Server.

Upgrading Parallels Mac Management for Microsoft SCCM 2012

To upgrade Parallels Mac Management for Microsoft SCCM 2012 to a newer version, you need to uninstall the current version and then install a new one. To run the uninstaller, navigate to **Start** > **Control Panel** > **Programs** > **Uninstall a program**. Find **Parallels Mac Management for Microsoft SCCM 2012** in the list of installed programs and uninstall it. If you installed Parallels Mac Management components on different servers, you need to uninstall each component individually. Once that's done, you can install the new version of Parallels Mac Management for Microsoft SCCM 2012. Please note that after upgrading Parallels Mac Management, you need to upgrade Parallels Mac Client on each managed Mac. See **Upgrading Parallels Mac Client** (p. 49) for more information.

Configuring Configuration Manager Boundaries

In order to install Parallels Mac Client on Mac computers, you need to configure Configuration Manager Boundaries in the Configuration Manager console.

Boundary is a network location on the intranet that can contain one or more Macs that you want to manage. Macs are assigned as clients to a Microsoft System Center Configuration Manager 2012 site according to the boundaries configured in the Configuration Manager console.

To create new or modify an existing boundary:

1. In the Configuration Manager console, navigate to **Administration / Overview / Hierarchy Configuration / Boundaries**.
2. To create a new boundary, right-click **Boundaries** and click **Create Boundary**. To modify an existing boundary, right-click it and select **Properties** from the pop-up menu.
3. On the **General** tab page of the boundary properties window, select the desired boundary type and specify its value(s) so that the Macs are located within the boundary. Please note that Parallels Mac Management supports the following boundary types:
   - IP subnet
   - IP address range
   - Active Directory site

After you create a boundary, you need to create a boundary group and add the boundary to it.

To create a new or modify an existing boundary group:

1. In the Configuration Manager console, navigate to **Administration / Overview / Hierarchy Configuration / Boundary Groups**.
2. To create a new boundary group, right-click **Boundary Groups** and click **Create Boundary Group**. To modify an existing boundary, right-click it and select **Properties** from the pop-up menu.

3 On the **General** tab of the boundary group properties window type in the boundary name and an optional description.

4 Click the **Add** button and select a boundary from the list. Click **OK**.

5 On the **References** tab page, select the **Use this boundary group for site assignment** option.

6 Select your site in the **Assigned site** drop-down box.

7 In the **Content location** section, click the **Add** button and select a site system server to associate with this boundary group. Click **OK**.

8 Click **OK** to save the boundary group and close the window.

Configuring Windows Firewall

To enable Configuration Manager Proxy and NetBoot Server network communications, their executable files must be added to the Windows firewall exception list.

The name and path of the Configuration Manager Proxy executable is:

```
%ProgramFiles(x86)%\Parallels\Parallels Mac Management for Microsoft
SCCM\pma_isv_proxy_service.exe
```

The name and path of the NetBoot Server executable is:

```
%ProgramFiles(x86)%\Parallels\Parallels Mac Management for Microsoft
SCCM\pma_netboot_service.exe
```

To add the executables to the Windows firewall exception list, open the Windows Control Panel and click (or double-click) Windows Firewall. Depending on the version of Windows, use the corresponding Windows Firewall dialog to add the `.exe` files to the list of programs allowed through Windows Firewall.

For the list of ports used by Parallels Mac Management for Microsoft SCCM 2012, see **Ports Used by Parallels Mac Management** (p. 147).

Viewing Proxy Service Certificate Details

The account that you use to run the Configuration Manager Proxy service must have permissions to access the certificate store on the local computer and to read the Configuration Manager Proxy certificate private key. The permissions are set automatically when you run the Configuration Manager Proxy Configuration Wizard and specify the account for running the service. If you're having a problem accessing Macs from the Configuration Manager console, you can check that the certificate permissions are valid for the account that you use to run the Configuration Manager Proxy service.

To view the certificate store permissions

1. Run regedit.exe on the computer where the Configuration Manager Proxy is installed.
2. Navigate to **HKLM\Software\Microsoft\SystemCertificates**.
3. Right-click **SystemCertificates** and select **Permissions** from the pop-up menu.
4. In the **Permissions for SystemCertificates** dialog, verify that the user that you use to run the Configuration Manager Proxy service has the **Read** permission selected.

To verify that the Configuration Manager Proxy service account has permissions to read the certificate private key

1. Open the Microsoft Management Console (MMC) from the **Start** menu by clicking **Run** and then typing "mmc".
2. In the **File** menu, select **Add/Remove Snap-in...**
3. In the **Add or Remove Snap-ins** dialog, find and select Certificates in the **Available snap-ins** list. Click **Add**.
4. In the **Certificate snap-in** dialog, select **Computer account** and then select **Local computer**.
5. Click **OK** in the **Add or Remove Snap-in** dialog.
6. In the snap-in tree, navigate to **Certificates (Local Computer)\Personal\Certificates** and expand it to view the available certificates.
7. Make sure that the **Configuration Manager Proxy** certificate exists. If it doesn't, run the Configuration Manager Proxy configuration utility.
8. Right-click the **Configuration Manager Proxy** certificate, point to **All Tasks**, and then click **Manage Private Keys**.
9. In the **Permissions for Configuration Manager Proxy private keys** dialog, verify that the user (or a group to which the user belongs) has **Read** access to the certificate's private key.

Note: To view certificates on Windows versions prior to Windows Server 2008, use a resource kit utility winhttpcertcfg.exe.

Migrating Configuration Manager Proxy

This section describes how to migrate the Configuration Manager Proxy to another server on the same Configuration Manager site.

To migrate the Proxy to another server, you need to:

1. Export the Configuration Manager Proxy certificate from the Windows Certificate Store on the current server.
2. Uninstall the Configuration Manager Proxy from the current server.
3. Import the certificate into the Windows Certificate Store on the new server.

4 Install the Configuration Manager Proxy on the new server.

The following describes how to export the existing certificate and import it on a new server. The Proxy uninstallation and installation should be performed normally, as described in **Install Parallels Mac Management for Microsoft SCCM 2012** (p. 31).

Exporting Certificate from Certificate Store

To export a certificate:

1 In Windows, click **Start** > **Run...**

2 Type `mmc` in the **Open** box. This will open the Microsoft Management Console.

3 In the console, click **File** > **Add/Remove Snap-in** to open the **Add or Remove Snap-ins** dialog.

4 Click **Certificates** in the **Available snap-ins** list.

5 Click the **Add** button. Select the **Computer account** option and click **Next**.

6 On the **Select Computer** page, select **Local computer** and click **Finish**. Click **OK** to close the **Add or Remove Snap-ins** dialog.

7 In the Microsoft Management console, click **Console Root / Certificates(Local computer) / Personal / Certificates**.

8 Right-click the Parallels Configuration Manager Proxy certificate and then click the **All Tasks > Export...** option in the pop-up menu. The **Certificate Export Wizard** opens.

9 Click **Next** on the **Welcome** page.

10 Select **Yes, export the private key** and click **Next**.

11 On the **Export File Format** page, select the following options:

- **Personal Information Exchange - PKCS #12 (.PFX)**
- **Include all certificates in the certification path if possible**
- **Export all extended properties**

12 Click **Next**.

13 On the **Password** page, type and confirm a password (you'll be asked for it when importing the certificate on the new server). Click **Next**.

14 Type a path and filename for the target certificate file (e.g. `C:\sccm_proxy.pfx`) and click **Next**.

15 Review the export summary and click **Finish** to complete the wizard.

16 Copy the certificate file to the server where you want to migrate the Configuration Manager Proxy.

Importing Certificate into Certificate Store

To import a certificate:

1. In Windows, click **Start** > **Run...**
2. Type `mmc` in the **Open** box and click **OK**. This will open the Microsoft Management Console.
3. In the console, click **File** > **Add/Remove Snap-in** to open the **Add or Remove Snap-ins** dialog.
4. Click **Certificates** in the **Available snap-ins** list.
5. Click the **Add** button. Select the **Computer account** option and click **Next**.
6. On the **Select Computer** page, select **Local computer** and click **Finish**.
7. Click **OK** to close the **Add or Remove Snap-ins** dialog.
8. In the Microsoft Management console, click **Console Root / Certificates(Local computer)**.
9. Right-click the **Personal** node and then click the **All Tasks > Import...** item in the pop-up menu. The **Certificate Import Wizard** opens.
10. Click **Next**.
11. On the **File to Import** page, click the **Browse** button and select the ".pfx" certificate file that you exported earlier (make sure to change the filter in the **Open** dialog to `.pfx`). Click **Next**.
12. On the **Password** page, type the password that you entered when you exported the certificate and select the **Mark this key as exportable...** option.
13. Click **Next**.
14. On the **Certificate Store** page, select the **Place all certificates in the following store** option. Make sure that the **Certificate store** field is set to **Personal** (if it doesn't, click the **Browse** button and select **Personal** from the list).
15. Click **Next**.
16. Review the import summary and click **Finish** to complete the wizard.
17. Install and configure Configuration Manager Proxy on the new server by running the Parallels Mac Management for Microsoft SCCM installation program.
18. The Mac computers will automatically discover the new Configuration Manager Proxy and will update their local Proxy connection records. For more information, please see **Updating Proxy Connection URL** (p. 48).

CHAPTER 3

Deploying Parallels Mac Client

After Parallels Mac Management for Microsoft SCCM 2012 has been installed and configured, you need to install the Parallels Mac Client software on Mac computers that you want to manage.

The client software can be installed on Mac computers using one of the following methods:

- **Deploying via Network Discovery.** This method scans your network for Mac computers and automatically adds them to the Configuration Manager site database. Network discovery can also perform a client push installation and enroll the Mac in Configuration Manager.
- **Using an interactive installer**. This type of installation is done by running an installer with a graphical user interface.
- **Using an installation script**. This installation option allows to install the Mac client from the command line. The script can be executed manually on each Mac or it can be distributed to and executed on Macs using Apple Remote Desktop or a similar remote management software.

The following topics describe how to use each installation method.

In This Chapter

Deploying Mac Client via Network Discovery 41
Installing Mac Client Using Interactive Installer 44
Installing Mac Client Using Installation Script 46
Configuring Mac OS X Firewall 47
Verifying Mac Client Deployment 48
Updating Parallels Configuration Manager Proxy Connection URL..... 48
Upgrading Parallels Mac Client 49
Uninstalling Parallels Mac Client..... 49

Deploying Mac Client via Network Discovery

Network discovery is a feature that finds Mac computers on your network and automatically adds them to the Configuration Manager site database. Network discovery can also perform a client push installation and assign discovered Macs to the Configuration Manager site. Use the instructions provided in this section to learn how to configure and use Parallels Mac Management network discovery.

Configuring Network Discovery

To configure network discovery:

1. In the Configuration Manager console, navigate to **Administration / Overview / Parallels Mac Management / Discovery Methods**. The list in the right pane will be populated with one or more "Parallels Network Discovery" entries according to the following:
   - If you don't have secondary sites, the list will contain just one Parallels Network Discovery entry.
   - If you have secondary sites but you've installed the Configuration Manager Proxy only on the primary site, the list will contain just one entry.
   - If you have secondary sites and installed the Configuration Manager Proxy on the primary and a secondary site, the list will contain an entry for each site where the Proxy is installed. The site name is displayed in the **Site** column.
2. Right-click the Parallels Network Discovery entry for the desired site and then select **Properties**. The **Parallels Discovery Properties** dialog opens.
3. Use the **General** tab page to configure general settings:
   - Use the **Enable network discovery** option to enable or disable network discovery.
   - Use the controls in the **Nmap scan settings** section to specify the Network Mapper settings. You can specify the TCP ports to scan (separated by a comma, space, or semicolon) and select the Nmap timing policy. The timing policy list contains the standard Nmap timing options ranging from the nearly invisible "paranoid" to the aggressive "insane" option. The default Nmap settings provide the optimal balance between the quality of the results and the time it takes to scan the network. If you believe that these settings will not yield the best results in your particular situation, you may fine tune them according to your needs.
4. Use the **Accounts** tab page to specify user accounts that will be used to install client software on Mac computers. You can specify more than one account. The accounts will be used by discovery in the order listed. This step is necessary only if you want to perform the client push installation. If you don't specify any accounts, network discovery will add the discovered Macs to the Configuration Manager as unmanaged resources. Use the following guidelines when specifying the accounts:
   - If Mac computers in your organization are members of a domain, you can specify a domain administrator account.
   - If the Macs are not members of a domain, you can specify accounts that have administrative privileges on their respective Macs. You also need to enable SSH access on each Mac. To do so, in Mac OS X, open **System Preferences > Sharing**. Find the **Remote login** service in the list and enable it. Add the user with administrative privileges to the list of users who are allowed SSH access.

5 Use the **Boundaries** tab page to specify Configuration Manager boundaries to search. You can use this search option together with the options on the **Subnets** tab page, but searching boundaries should be the primary method. If you haven't configured boundaries and boundary groups yet, you need to configure them before using this option (p. 36).

   The **Boundaries** tab page has the following elements:

   - **Boundary Groups to search** list — Lists boundary groups. The groups displayed here are the groups that are used for the current site assignment (the **Use this boundary group for site assignment** option is selected in the boundary group **Properties** dialog). The groups that are not associated with any site are included in the list too. Highlight the group to display individual boundaries in the list below it. To search all boundaries in the group, select the check-box in front of the group name.
   - **Boundaries to search** list — Lists boundaries that belong to the highlighted boundary group. Select the boundaries to search.
   - **Quick filter** — Allows to specify a filter for the **Boundaries to search** lists. You can type any part of the text that might appear in the boundary's name, type, or description.

6 Use the **Subnets** tab page to specify the subnets to search. You can search subnets if you can't search boundaries (described above) for any reason. Select **Search local subnets** to search local subnets. To search other subnets (in addition to or instead of the local subnets), click the New icon and then in the **New Subnet Assignment** dialog, enter the **Subnet** and **Mask** information. Make sure that the **Enable subnet search** check box is selected and then click **OK**. Use the provided icons to Edit, Delete, and Enable/Disable a subnet scan.

7 On the **Schedule** tab, click the New icon to set a schedule for running discovery. The **Custom Schedule** dialog opens:

   - Set the start date and start time for a discovery run.
   - Set the discovery duration. This setting specifies the maximum length of time for a discovery run. If all resources are discovered before this time is up, the run will continue with minimal network traffic until this time is up. If the run is not completed before this time is up, only the resources already discovered will be included in the result.
   - In the **Recurrence pattern** group box, select how this schedule will recur. The following choices are available:

     None: The scheduled run is a one-time-only event.

     Weekly: The scheduled run will occur weekly at the same start time.

     Monthly: The scheduled run will occur monthly at the same start time.

     Custom Interval: The scheduled run will occur at a custom interval set by the administrator.

8 Click **OK**, and then click **OK** again.

Running Network Discovery

Network discovery runs on a schedule as specified in the discovery configuration (see above). A discovery run will perform the following actions:

1. When discovery finds a Mac, it will try to connect to it over SSH using user accounts that you specified in the discovery configuration. The accounts will be used in the order listed. If you haven't specified any accounts (or if a connection with the Mac cannot be established for any reason), the Mac will be added to the Configuration Manager site as an unmanaged resource. In such a case, the rest of the steps in this list will not be performed.
2. Once discovery establishes a connection with the Mac, it will push the client software installation package to it and will continue to scan the network.
3. The installer will install the client on the Mac and will register it with the Configuration Manager Proxy. As a result, the Mac will be assigned to the Configuration Manager site as a managed resource.

In a situation when a discovered Mac has the client software already installed, the following scenarios will be considered:

- If the client is registered with a different Configuration Manager Proxy but reports the same Configuration Manager site code as the current site, the client is re-registered with the current Configuration Manager Proxy and the Mac remains to be managed on the current site. This scenario may occur when you re-install the Configuration Manager Proxy on your Configuration Manager site (e.g. install in on a different computer).
- If the client is registered with a different Configuration Manager Proxy and reports a different site code, the client registration remains unchanged and the Mac is ignored by discovery. This situation may occur when a Mac computer (e.g. a laptop) is managed by Parallels Mac Management in one organization and is brought in to another organization that also uses Parallels Mac Management to manage their Macs. The site code comparison allows to prevent a situation when a Mac is added by mistake to a wrong Configuration Manager site.

The discovered Macs (both managed and unmanaged) are placed into the **All Mac OS X Systems** collection. Please note that if you have secondary sites, the Macs within their scope will be placed into the same **All Mac OS X Systems** collection on their respective primary site. For more information, see **Collections in Parallels Mac Management** (p. 57).

Installing Mac Client Using Interactive Installer

This section describes how to install Parallels Mac Client on a Mac using the installation program with a graphical user interface.

To download the installation program to a Mac computer:

1. Make sure that the Configuration Manager Proxy service is installed and running.
2. Log in to a Windows server running the Configuration Manager console.
3. In the Configuration Manager console, navigate to **Administration** / **Overview** / **Parallels Mac Management**.
4. Click **Mac Client Enrollment**. The list in the right pane will be populated with one or more Mac Client Enrollment entries according to the following:

- If you don't have secondary sites, the list will contain just one "Mac Client Enrollment" entry.
- If you have secondary sites but you've installed the Configuration Manager Proxy only on the primary site, the list will contain just one entry.
- If you have secondary sites and installed the Configuration Manager Proxy on the primary and a secondary site, the list will contain an entry for each site where the Proxy is installed. The "Site" column contains the name of the site.

5 Right-click the Mac Client Enrollment entry that corresponds to the site where the Macs are located and click **Properties**. **The Parallels Mac Management Properties** dialog opens.

6 Copy the URL from the Mac Client Installer URL field. The URL will look similar to the following:

`http://myhost.local:8761/files/pma_agent.dmg`

The installation image resides on the computer where the Configuration Manager Proxy is installed. In addition to its primary function (being a proxy) the Configuration Manager Proxy also acts as an HTTP server, so the installer can be downloaded from it to a Mac using a Web browser.

7 On a Mac, enter the URL into a Web browser to download the `pma_agent.dmg` image.

Once you've downloaded the installation image file, you can install the software on a Mac as follows:

1 Double-click the `pma_agent.dmg` file to open the image.

2 In the **Parallels Mac Management** window, double-click the **Parallels Mac Management.pkg** icon. This will start the installation assistant.

3 Follow the onscreen instructions. When asked, provide the Mac user name and password. The user must be allowed to administer this Mac.

4 On successful installation you should see the following message: "The installation was successful". Click **Close** to exit the installation assistant.

5 After you close the installation assistant, another assistant will automatically open. This assistant will register the Parallels Mac Management that you've just installed on your computer with Configuration Manager. Read the information provided on the **Introduction** page and then click **Continue**.

6 On the **Authorization** page, enter your company's domain name, your domain user ID and password.

7 Click **Continue**.

8 On successful registration you should see a confirmation message. If you receive an error, click the **Try Again** button to return to the Authorization page and re-enter the information. The registration may fail for the following reasons:

- The specified domain name and/or domain credentials are incorrect.
- The Mac IP address falls outside the boundary defined in Configuration Manager.
- The Configuration Manager Proxy service is not running.

If you close the wizard without completing the registration, it will run automatically at predefined intervals (5-10 minutes) and every time you restart the Mac. To stop this from happening, either resolve the problem and register the client with the Configuration Manager Proxy or uninstall it from the Mac (p. 49).

If firewall is enabled in Mac OS X, a message box will open at the end of a successful registration asking you if pma_agent.app should be allowed to accept incoming connections. Click **Allow**. This will add pma_agent.app to the firewall list of application that are allowed incoming connections.

The results of a successful client registration should be as follows:

- The Mac is assigned to the Configuration Manager site.
- The Mac inventory is collected and saved in the Configuration Manager database.
- The Mac is added to the **All Mac OS X Systems** collection in the Configuration Manager console.

Once installed, the Client will run on a Mac in the background and will start automatically every time the Mac OS X is restarted.

Installing Mac Client Using Installation Script

A special script is supplied with Parallels Mac Management that you can use to perform an unattended Mac client installation.

To obtain and use the script, follow these steps:

9 On a Windows server running Configuration Manager Proxy, navigate to the `C:\Program Files (x86)\Parallels\Parallels Mac Management for Microsoft SCCM\files` directory.

10 Locate the `InstallAgentUnattended.sh` file. This is the Mac client installation script. The script must be run on each Mac computer you want to enroll in Configuration Manager. You can copy the file to each Mac (e.g. copy it to a location from which Macs can download it) or you can use Apple Remote Desktop to run the script on the Macs remotely.

11 Please note that you must use `sudo` to run the script because the Mac client registration process requires superuser privileges.

When you run the script, provide the following parameters (in the order listed):

- `agent_download_url` — the URL of the Mac client installer (`pma_agent.dmg`). The URL can be obtained in the Configuration Manager console as described in the **Using Installation Program to Install Mac Client** section.
- `user_name` — this is the name of a domain user account that will be used to register the client with the Configuration Manager Proxy.
- `user_password` — the domain user password.
- `domain_name` — your company's domain name.

Example:

```
$ sudo ./InstallAgentUnattended.sh http://myhost.local:8761/files/pma_agent.dmg
myname mypass mydomain
```

If you receive the "Permission denied" error when executing the script, run the following command to set the file permissions and then execute the script again:

```
$ chmod 755 InstallAgentUnattended.sh
```

If you wish, you can hard code the URL, user/password, and the domain parameter values in the script, so you (or your Mac users) don't have to enter them in the command line. To hard code the parameter values, open the script in an editor and change the values of the input parameters from `$1`, `$2`, `$3`, `$4` to the desired values. The parameter names in the script are self-explanatory. Once the script is ready, give it to your Mac users, so they can execute it on their Macs, or use Apple Remote Desktop to execute it on Macs remotely.

When the script runs on a Mac, it displays the information in the console about the processes that it's running. When the script completes executing, it returns a numeric code. To see the return code, run the following command after the scrip finished executing:

```
$ echo $?
```

The "0" code returned by the above command indicates that the Mac client has been installed and registered properly. Any other code indicates a failure (you can also read the last messages in the console to get an idea of what went wrong).

Configuring Mac OS X Firewall

When the client software is installed on a Mac, the firewall in Mac OS X must be configured to allow client network communications. When the client is installed on a Mac manually, the Mac user will be asked if pma_agent.app should be allowed to accept incoming connections. The user can answer "Allow" or "Deny". The same message is displayed to a Mac user when the client push installation is performed by network discovery. If the user answers "Deny", the client will have to be added to the firewall exception list later as described below.

To add the client to the firewall exception list:

1. From the Apple menu, select **System Preferences**. The **System Preferences** dialog opens.
2. Select **Security & Privacy** and then click the **Firewall** tab.
3. If the firewall is running, the green light indicator will be "on" and its label will read "Firewall: On".
4. Click **Advanced**. The advanced firewall setting dialog opens.
5. Click the **+** icon. The Mac directory tree dialog opens.
6. In the directory tree, navigate to the `/Library/Parallels` folder and select the `pma_agent.app` file.
7. Click **Add** and then click **OK**.
8. Close the **System Preferences** window.

Verifying Mac Client Deployment

To verify that the Parallels Mac Management deployment was successful, open the Configuration Manager console and navigate to **Assets and Collections** / **Devices** / **All Mac OS X Systems**. You should see some Mac computers in the list. If you ran Network Discovery to discover Macs, some of those Macs may not have Parallels Mac Client installed on them. The possible reasons for this are described in **Deploying Mac Client via Network Discovery** (p. 41). To see if a Mac has Parallels Mac Client installed and running on it, look at the **Client** and **Client Activity** properties, which should say "Yes" and "Active" respectively. If the **Client** property says "No", it means that the Mac cannot be managed in SCCM because Parallels Mac Client is not installed on it. If the **Client Activity** property says "Inactive", the Mac may be turned off, disconnected from the network, or it may have some other issues that prevent the Configuration Manager to communicate with it.

Updating Parallels Configuration Manager Proxy Connection URL

If you migrate the Parallels Configuration Manager Proxy to a different server, its connection URL record must be updated on managed Mac computers. Parallels Mac Client is capable of making this update automatically as described below.

The Mac Client running on a Mac connects to the Parallels Configuration Manager Proxy using the connection URL that it obtains from the Active Directory during the Parallels Mac Client installation. If at some point the client fails to establish a connection with the proxy, it will try to recover the connection as follows:

1. First, it will try to access DNS records for the location of the Configuration Manager Proxy. If it finds the new connection URL in DNS, it will use it to connect to the Configuration Manager Proxy.
2. If the location cannot be found in DNS at this time, the client will keep trying to connect to the proxy and to find the new location in DNS for a period of one week.
3. If after a week the connection still cannot be establish, a dialog box will be displayed in OS X asking the Mac user to enter the Active Directory credentials. The client will then connect to the Active Directory and try to retrieve the Configuration Manager Proxy connection URL from it. If succeeded, the client will use the URL to connect to the Configuration Manager Proxy. If it fails again, it will display an error message to the Mac user advising them to contact the system administrator.

For additional information about migrating the Configuration Manager proxy to a different server, please see **Migrating Configuration Manager Proxy** (p. 38).

Upgrading Parallels Mac Client

When you upgrade Parallels Mac Management for Microsoft SCCM, the Parallels Mac Client must also be upgraded on every Mac computer. This task can be accomplished by distributing the client installation package to Macs using the standard software distribution functionality of Configuration Manager.

To upgrade Parallels Mac Client on Mac computers, obtain the Parallels Mac Client installation image file as described in **Installing Mac Client Using Interactive Installer**. The client installation image can be distributed to Mac computers using the software distribution functionality. The **Software Distribution** section describes how to accomplish this task. When creating a program for the distribution package, the **Command Line** property should be specified as follows:

```
:pma_agent.dmg/Parallels Mac Management for Microsoft SCCM.pkg::
```

Please note that when you install Parallels Mac Client via software distribution, the client registration parameters will be inherited from the existing registration file, so you don't have to configure the client again.

If you need to upgrade Parallels Mac Client on a single Mac, you can do it manually:

1. On a Mac, uninstall the Parallels Mac Client which is currently installed on it (see **Uninstalling Parallels Mac Client** (p. 49)). This is a necessary step. Please note that when updating Parallels Mac Client using the software distribution functionality (described above), the client uninstallation is done automatically.
2. Download the Parallels Mac Client installation image and run the installation program as described in **Installing Mac Client Using Interactive Installer**.

Uninstalling Parallels Mac Client

To uninstall the Parallels Mac Client software from a Mac:

1. Click **Go > Go to Folder** in the OS X menu bar.
2. Type `/Library` and click **Go**.
3. Locate and open the **Parallels** folder.
4. In the **Parallels** folder, right-click the `pma_agent.app` file and click **Show Package Contents** in the pop-up menu.
5. Open the `Contents/MacOS` folder.
6. Double-click the `pma_agent_uninstaller.app` file to start the uninstallation assistant.
7. Follow the onscreen instructions to uninstall the Parallels Mac Client.

The Mac will remain in the Configuration Manager database, but its management will not be possible. You can reinstall the client on the Mac later to restore management functions.

CHAPTER 4

Managing Parallels Mac Client

After you install Parallels Mac Client on a Mac and register it with Parallels Configuration Manager Proxy, you can begin managing the Mac in Configuration Manager. The Parallels Mac Client itself can also be managed on the Mac where it is installed. This chapter describes the common Parallels Mac Client management tasks.

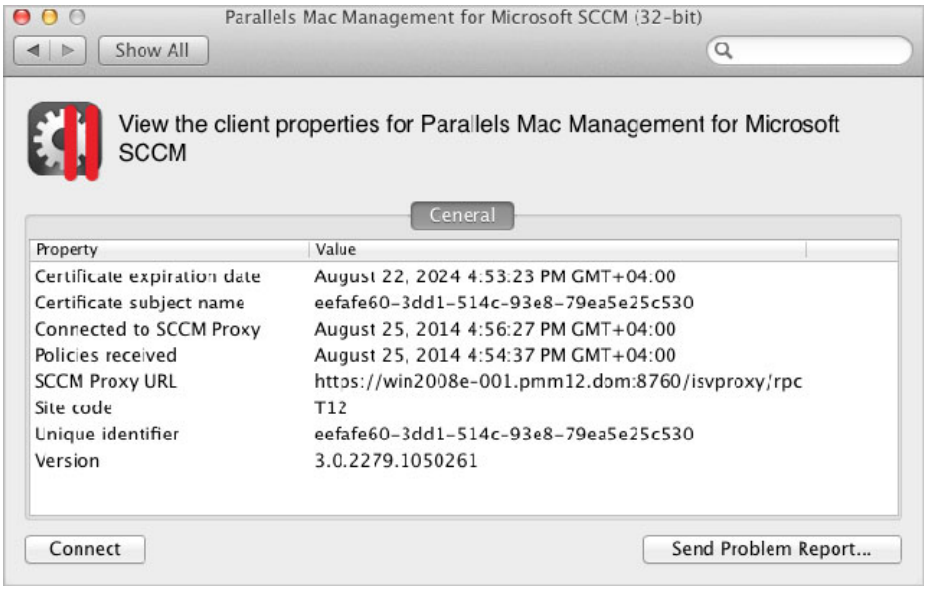
In This Chapter

Viewing Parallels Mac Client Properties 51
Initiating Policy Retrieval 53
Sending Problem Reports From Mac Client 55

Viewing Parallels Mac Client Properties

You can view the properties of the Parallels Mac Client installed on a Mac in the System Preferences application. In OS X, open System Preferences, then click the **Parallels Mac Management** icon. If System Preferences on a Mac are organized by categories, the icon is located in the **Other** category.

When you click the **Parallels Mac Management** icon, the following dialog opens:



The **General** box contains the Parallels Mac Client properties and their values:

- **Certificate expiration date**. The date and time when the Mac client certificate expires.
- **Certificate subject name**. A globally unique name identifying the Mac client for which the certificate was issued.
- **Connected to SCCM Proxy**. The last time the Parallels Mac Client established a connection with the Parallels Configuration Manager Proxy.
- **Policies received**. The last time the Parallels Mac Client downloaded its policy.
- **SCCM Proxy URL**. The URL of the computer where the Parallels Configuration Manager Proxy is running. This is the Parallels Configuration Manager Proxy with which this Parallels Mac Client is registered.
- **Site code**. The code of the Configuration Manager site to which this Mac is assigned.
- **Unique identifier**. A globally unique ID assigned to this Parallels Mac Client instance.
- **Version**. The Parallels Mac Client version number.

The buttons at the bottom of the dialog are:

- **Connect**. Click this button to download the latest Mac client policy from the Configuration Manager. For more information, please read **Initiating Policy Retrieval for a Mac Client** (p. 53).
- **Send Problem Report**. Click this button to send a problem report to Parallels Support. For more information, please read **Sending Mac Client Problem Report** (p. 55).

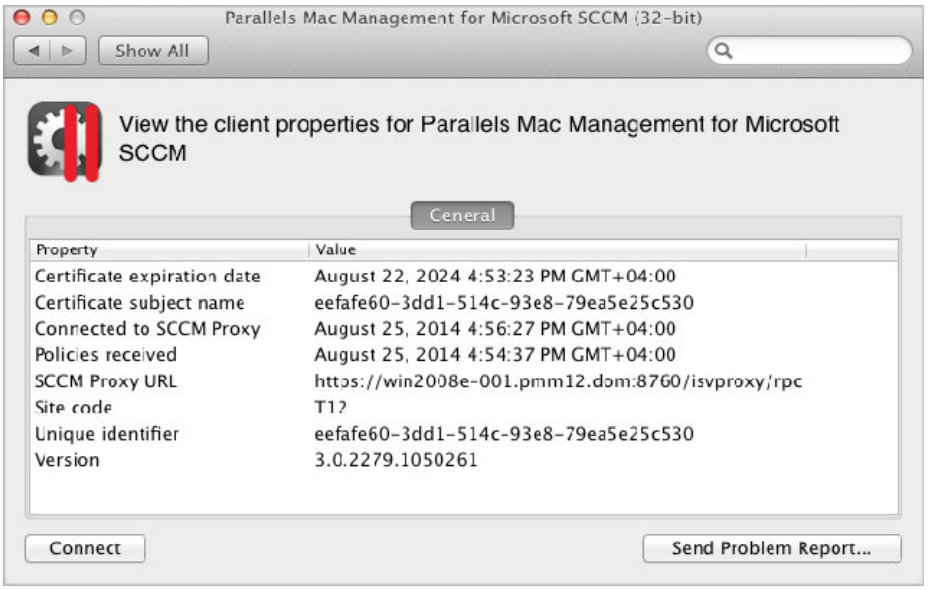
Initiating Policy Retrieval

Parallels Mac Client downloads its policy from Configuration Manager automatically according to a schedule. There may be a need to download the latest policy before the scheduled download occurs. Parallels Mac Client provides this ability.

Using Graphical User Interface to Initiate Policy Retrieval

To initiate manual policy retrieval, open System Preferences, then click the **Parallels Mac Management** icon.

The following dialog opens:



Click the **Connect** button to initiate policy retrieval. A text will appear next to the **Connect** button informing you of the progress. Once the operation is completed, the text will describe the result. If the connection to Configuration Manager was successful, the text will say "Connected" and will specify how many policy updates were received. If there were no policy updates, the text will say "No policy updates". The **Policies received** property in the **General** list box will be updated if at least one update was received; it will remain unchanged if no updates were available.

Using Command Line to Initiate Policy Retrieval

To initiate policy retrieval from a command line, change directory to `/Library/Parallels/pma_agent.app/Contents/MacOS` and type the following command in Terminal:

```
$ pmmctl get-policies
```

On completion, the command returns one of the following XML documents depending on the result:

Policy retrieval failed

```
<plist version="1.0">
    <dict>
        <key>ErrorCode</key>
        <integer>3</integer>
        <key>ErrorMessage</key>
        <string>Operation timed out</string>
    </dict>
</plist>
```

where the `<integer>` element contains the error code, and the `<string>` element contains the error description.

Policy retrieval was successful

```
<plist version="1.0">
    <dict>
        <key>ErrorCode</key>
        <integer>0</integer>
        <key>ErrorMessage</key>
        <string>No error</string>
       <key>NumberOfPolicyUpdates</key>
       <integer>5</integer>
    </dict>
</plist>
```

where the `<integer>` value of the `<NumberOfPolicyUpdates>` key contains the number of policy updates retrieved.

To obtain the list of possible error codes with descriptions, use the following command:

```
$ pmmctl error-info
```

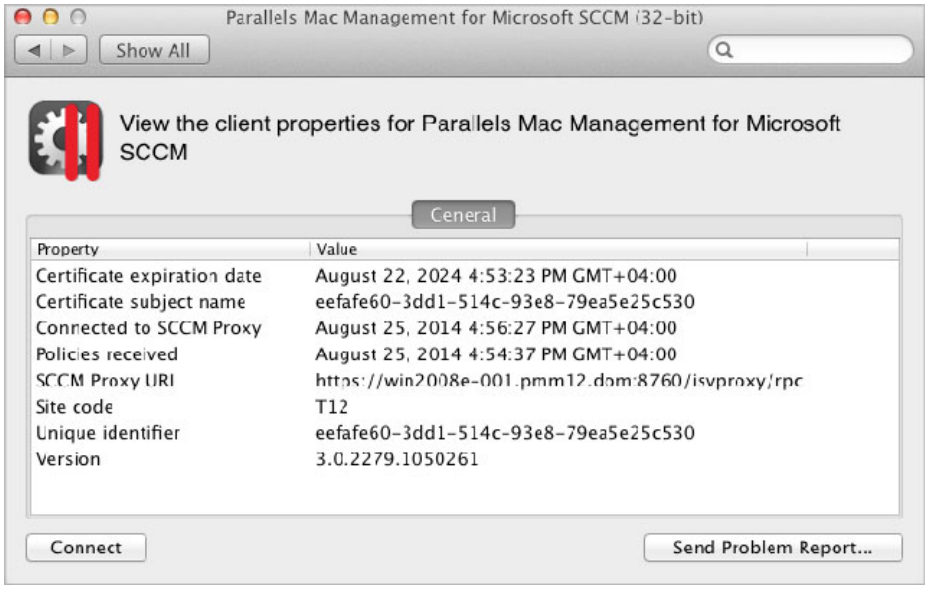
The command returns the following list:

```
0: No error
1: Invalid command
2: Operation failed
3: Operation timed out
4: Connection aborted
5: Unknown error code 5
```

Sending Problem Reports From Mac Client

If you are experiencing a problem with Parallels Mac Client, you can obtain a problem report and then send it to Parallels Support. To obtain a report, open **System Preferences** and then click the **Parallels Mac Management** icon.

The following dialog opens:



Click the **Send Problem Report** button to obtain a report. The **Send Problem Report** dialog opens and the report data gathering process begins. Once the report file is generated, a message is displayed in the dialog specifying its location on the local hard drive. Clicking the **Send** button will send the report to the Parallels Configuration Manager Proxy, which will notify the IT administrator through the Problem Monitoring utility (p. 113). The Problem Monitor can then be used to view the report summary and to send it to Parallels Support.

The problem reporting utility can also be run from Finder as follows:

1. Open Finder and navigate to the `/Library/Parallels/` folder.
2. Locate the `pma_agent.app` package, right-click it and select **Show Package Contents**.
3. In the package, navigate to the `Contents/MacOS` folder and double-click the `pma_report_tool` file. The **Send Problem Report** dialog opens.

This is the same dialog as the one that opens when you click the **Send Problem Report** button described above.

CHAPTER 5

Parallels Mac Management Features

This chapter contains information about how to use Parallels Mac Management features.

In This Chapter

Using Configuration Manager 2012 Console 57
Understanding Collections in Parallels Mac Management 57
Hardware and Software Inventory 58
Desired Configuration Management 59
Application Management 88
Software Distribution 97
Deploying Mac OS X Images 101
Deploying Parallels Desktop and Virtual Machines on Macs 105
Deploying SCCM Client in Windows Running in a Virtual Machine 107
Providing Remote Assistance to Mac Users 109
Problem Reporting and Monitoring 111

Using Configuration Manager 2012 Console

Parallels Mac Management extends the Configuration Manager 2012 console with support for Mac OS X systems. The Configuration Manager console is the primary interface to manage Mac computers in your enterprise. After you install Parallels Mac Management, the Mac-specific GUI elements become available in the console allowing you to accomplish day-to-day Mac management tasks.

Understanding Collections in Parallels Mac Management

Configuration Manager 2012 collections help system administrators to manage resources by combining them into logical groups based on a certain criteria. Parallels Mac Management adds the **All Mac OS X Systems** collection to organize Mac computers.

To see the **All Mac OS X Systems** collection, open the Configuration Manager 2012 console and navigate to **Assets and Compliance / Overview / Device Collections / All Mac OS X Systems**. The collection can contain both managed and unmanaged Macs. A Mac is added to a collection as an unmanaged resource if the client software is not installed on it or if it's not registered with the Configuration Manager Proxy. You can still view the properties of an unmanaged Mac and connect to it using SSH or VNC if needed.

To identify managed and unmanaged Mac resources in the **All Mac OS X Systems** collection:

1. Right-click a resource and select **Properties** from the pop-up menu.
2. In the **Properties** dialog, select the **General** tab.
3. In the **Discovery data** list, look up the "Client Version" property:
   - The client version of a managed resource will contain the Parallels client software version number followed by "-PMA". For example: "5.1.6.804674-PMA".
   - The client version of an unmanaged resource will be "Unknown-PMA".

The **All Mac OS X Systems** collection uses the following criteria in the `WHERE` clause of its SQL statement:

```
ClientVersion LIKE '%-PMA'
```

Therefore, the Mac resources that have the client version ending with "PMA" are displayed in the **All Mac OS X Systems** collection. You can create your own collections for Mac resources using a different criteria if needed.

Hardware and Software Inventory

When Mac computers are enrolled in Configuration Manager, the hardware information is collected from them and is saved in the Configuration Manager database. Hardware inventory provides system information such as processor type, available disk space, network interfaces, etc. You can also view the list of installed Mac OS X applications as part of the hardware inventory data.

Configuring Inventory Settings

To configure Software Inventory settings:

1. In the Configuration Manager console, navigate to **Administration / Client Settings.**
2. Right-click the **Default Client Settings** item and then click **Properties**.
3. In the **Default Settings** dialog, select the **Client Policy** item in the left pane and use the **Client policy polling interval (minutes)** option to configure the policy polling interval. Please note that the values specified in this dialog apply to both managed Windows and managed Mac computers.
4. To configure Hardware Inventory settings:

5 In the **Default Settings** dialog, select **Hardware Inventory** in the left pane.

6 Use the controls in the right pane to enable and schedule hardware inventory.

7 To select the classes to be collected by hardware inventory, click the **Set Classes** button. Review the selected classes and make changes if needed. Please note that Parallels Mac Management adds the **Apple Warranty Info (PMM_AppleWarrantyInfo)** custom class and automatically selects it for the **Default Client Settings** entry. The class collects the Apple warranty information of Mac computers. For more info, see **Tracking Apple Warranty Status of Macs** (p. 116).

Viewing Inventory Data

To view hardware and software inventory data for a Mac computer:

1 Open the collection containing Mac resources (e.g. **All Mac OS X Systems**).

2 Right-click a Mac of interest and select **Start > Resource Explorer** in the context menu.

3 The **Resource Explorer** snap-in opens where you can browse the resources and view inventory items for them.

Desired Configuration Management

Parallels Mac Management extends the Configuration Manager 2012 Desired Configuration Management (DCM) by adding the ability to define and enforce corporate policies for Mac OS X computer configurations. Using this feature you can track and rectify the configuration compliance of client Macs in your organization.

Parallels Mac Management provides the functionality to monitor and enforce the following:

- **OS X Configuration** (p. 59)
- **FileVault 2 Encryption** (p. 66)
- **Parallels Desktop Preferences** (p. 79)
- **Parallels Desktop Virtual Machine Settings** (p. 81)

In addition, you can use the standard **Create Configuration Item Wizard** (p. 82) where you can define scripts to assess arbitrary settings on client Macs and to remediate noncompliant values.

Deploying OS X Configuration Profile

Parallels Mac Management for Microsoft SCCM 2012 provides the functionality to monitor and enforce OS X configuration settings on managed Mac computers. To do so, you need to define a desired OS X configuration profile and then deliver it to Macs using the DCM functionality. A Mac receiving the profile is evaluated for compliance and the necessary changes are made to the noncompliant OS X configuration settings.

Parallels Mac Management provides two methods of defining an OS X configuration profile:

- Using a custom configuration item dialog in the Configuration Manager Console to define a profile from scratch.
- Creating a profile from an existing file containing the OS X profile data. Such a file can be created in advance using Mac OS X Server's Profile Manager and then imported into the configuration item dialog designed for this purpose.

The following topics describe each method in detail.

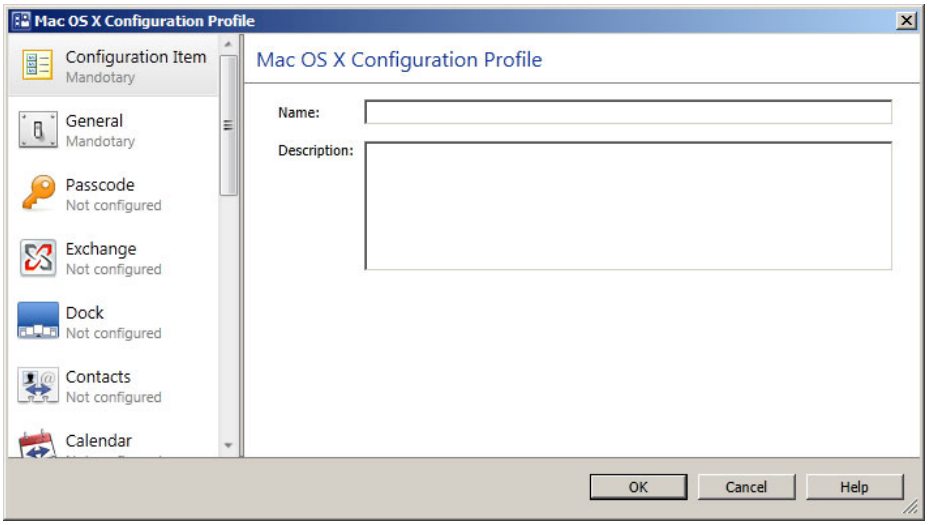
Creating OS X Configuration Profile

The **Mac OS X Configuration Profile** dialog is used to create a configuration item that allows you to deliver Mac OS X configuration profiles to managed Macs. A Mac receiving the profile is evaluated for compliance and the necessary changes are made to the noncompliant OS X configuration settings.

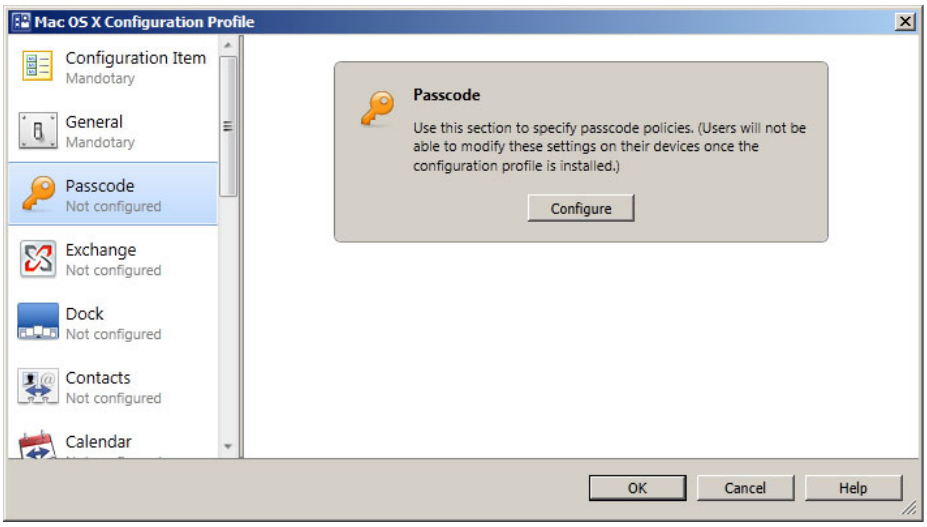
Parallels Mac Management provides two separate dialogs to create Mac OS X configuration items. The first dialog (described here) allows to define all of the OS X profile values right in the dialog itself. The second dialog (described in the section that follows this one) (p. 63) allows to create a configuration item from an existing file containing the OS X profile data. You can use either dialog depending on your needs.

To create a Mac OS X configuration item from scratch:

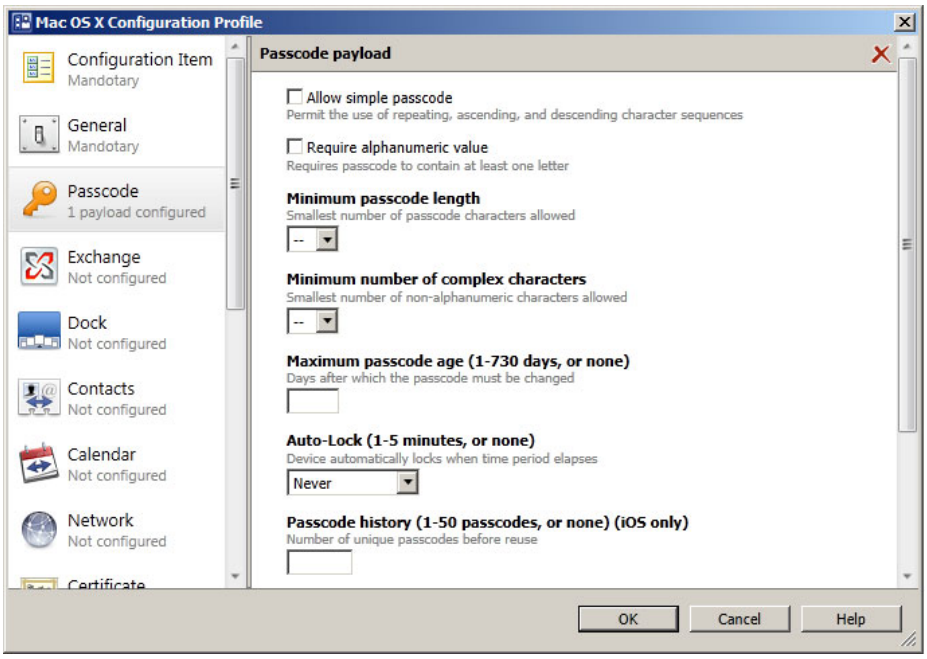
1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Items,** point to **Create Parallels Configuration Item,** and then click **Mac OS X Configuration Profile**.
3. The **Mac OS X Configuration Profile** dialog opens.



The dialog mimics the interface of the Mac OS X Server's Profile Manager. The left pane of the dialog contains the list of payloads that define groups of settings. The right pane contains the settings for a selected payload. When you select a payload for the first time, the right pane will only contain a short description and the **Configure** button.



Clicking the **Configure** button will show the actual editable fields.



Some of the items will be populated with the default values, some will be empty. If this is a new configuration profile, only the **Configuration Item** and the **General** payloads will show the editable fields. All others will contain just the **Configure** button. Specifying the values for a particular payload is optional. If you see only the **Configure** button and no editable fields, it means that the payload is currently excluded from the configuration profile and will not be evaluated. If you already specified the values and want to remove the entire payload from the profile, click the red **X** icon in the upper right hand corner.

Allowing Users to Specify Mac OS X Profile Settings Interactively

When setting up a Mac OS X profile for multiple users, it may not be possible to specify all of the settings in advance. For example, when configuring the Exchange payload, the user account, email address, and password must be specified individually for each user. In a case like this, you may allow Mac users to provide the required settings interactively when the profile is applied on a Mac.

Some of the editable fields on payload screens are marked in light gray as *required*, *set on device*, and *optional*. Required fields must have a value or you will not be able to save the profile. "Set on device" fields can be mandatory or optional and most likely should be set on an individual Mac (e.g. user names and passwords). Optional fields are optional. The logic that determines whether the profile is applied on a Mac interactively or silently is as follows:

- To use the interactive mode, enter the `%user_interaction_required%` tag into a field instead of the actual value. If a payload contains this tag in at least one field, a Mac user will be prompted to manually enter all of the missing settings. The interactive mode will be used even if none of the missing settings are actually required on the Mac OS X side. You can enter the `%user_interaction_required%` tag into any field that you want a user to set manually, including required, set-on-device, and optional fields.
- If a payload does not contain the `%user_interaction_required%` tag, an attempt will be made to apply the profile on a Mac silently. If the profile cannot be applied silently (one or more settings that are required on the Mac OS X side are missing), the interactive mode will be used and the user will have to specify them manually.

In the interactive mode, a standard System Preferences dialog will be opened in Mac OS X for each corresponding payload where the user will have to specify the required settings. The dialog has the **Install** and **Cancel** buttons. To apply the settings, the user clicks the **Install** button. If the specified values are invalid, the user will have to enter them again. On success, a report will be sent to SCCM. If the user clicks the **Cancel** button, the profile installation is aborted and an appropriate report is sent to the administrator.

Please also note that when you create a Mac OS X configuration profile using the Profile Manager, you have an option to set the **Profile Distribution Type** to **Automatic Push** or **Manual Download**. When you use the profile editor in the Configuration Manager console (described in this section), the distribution type is always **Manual Download**. The requirements for specifying certain settings are not as strict with the **Manual Download** distribution type.

Payload Overview

The first item in the payload list is **Configuration Item**. It is not really a payload and is used to specify the configuration item name and an optional description. This is the name that will appear in the **Configuration Items** list in the Configuration Manager console after you save the profile.

The **General** payload (second in the list) specifies the Mac OS X configuration profile general information.

The rest of the payloads specify the corresponding Mac OS X system preferences. The following list provides a general description of each payload. For the complete information about creating a Mac OS configuration profile, please refer to Apple's documentation.

Payload	Description
Passcode	Used to specify passcode policies.
Exchange	Exchange account configuration.
Dock	Dock item settings. Dock appearance settings.
Contacts	Contacts LDAP configuration (CardDAV).
Calendar	Calendar server account configuration (CalDAV).
Network	Network Interface (Ethernet or Wi-Fi).
Certificate	X.509 certificates.
Security & Privacy	Usage and diagnostic information opt-out.

Saving the Configuration Profile

When you are finished entering the configuration profile information, click the **OK** button. This will create a configuration item that will appear in the **Configuration Items** list in the Configuration Manager console. To view the configuration item data or to edit the profile, right-click it and select **Edit Parallels Configuration Item** from the pop-up menu.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

Creating OS X Configuration Profile from File

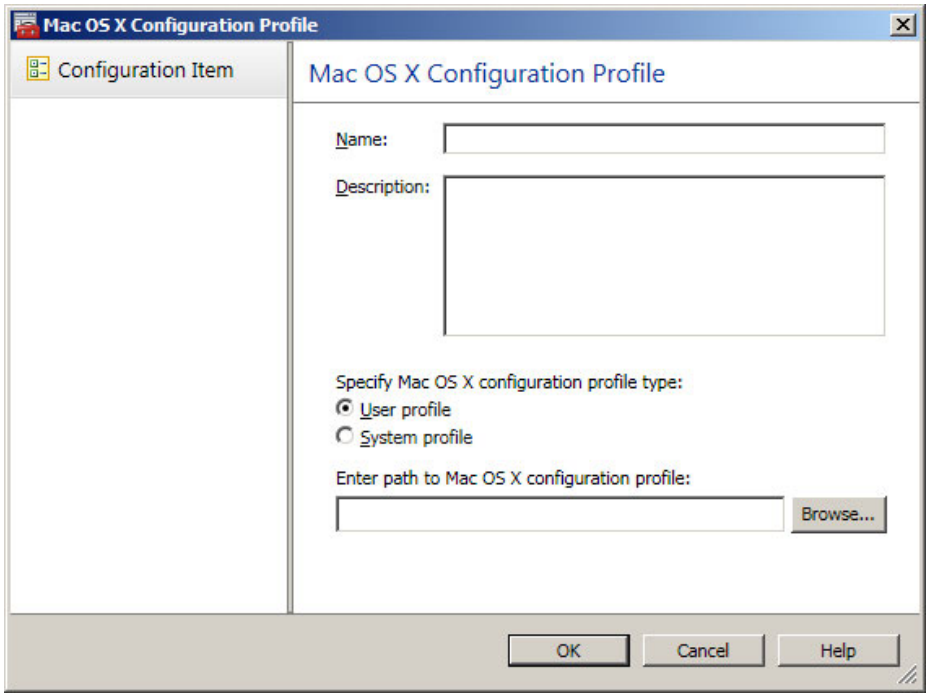
The previous section described how to create a Mac OS X configuration item from scratch using only the Configuration Manager console. Alternately, you can create a Mac OS X configuration item from an existing file containing the Mac OS X profile data. Such a file can be created using Mac OS X Server's Profile Manager. You can use this approach if you already have a profile created externally or if you prefer to use Profile Manager for any reason. For supplementary information, see **Using Profile Manager** at the end of this section.

To create a Mac OS X configuration item from a file:

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items** and then point to **Create Parallels Configuration Item** and click **Mac OS X Configuration Profile from File**.

3 The **Mac OS X Configuration Profile** dialog opens.



4 Enter the desired configuration profile name and description.

5 Select the profile type from the following options:

- **User profile**. Select this option if you want to install the configuration profile using the current user's security context.

  Note: The System Policy Control payload (designated by specifying `com.apple.systempolicy.control` as the `PayloadType`) must only exist in a device profile. If the payload is present in a user profile, an error will be generated during installation and the profile will fail to install.

- **System profile**. Use this option when you want to install the configuration profile as `root`.

6 Click the **Browse** button, locate and select the Mac OS X configuration profile file that you've created using Profile Manager (the file with the ".mobileconfig" extension), and click **Open**.

7 Click **OK** to save the configuration item. The new configuration item is created with the XML content of the configuration profile embedded into it. If the item doesn't appear in the **Configuration Items** list, right-click anywhere in the list and click **Refresh**.

8 To edit the profile data after the configuration item has been saved, right-click the profile and select **Edit Parallels Configuration Item** from the pop-up menu. The **Mac OS X Configuration Profile** dialog will now have the **Import from .mobileconfig** and **Export to .mobileconfig** buttons. Using these two buttons, you can export the profile into a file, edit it in an external application (e.g. Profile Manager) and then import it back into the configuration item.

   The import operation will perform the following validations of the profile data:

   - The profile type (User or System) must be the same as the original.
   - If this is a signed profile, the payload identifier must be the same as the original.
   - If the profile is not signed but the payload identifier differs from the original, a message box containing this information will be displayed. You'll have an option to cancel or continue the importing operation.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

Using Profile Manager

Profile Manager is a tool provided by Apple that allows to create a Mac OS X configuration profile (an XML file) containing the configuration settings that your organization requires. The configuration profile can then be deployed to Mac computers to configure them using the specified settings.

Note: You need a Mac OS X Server computer to use Profile Manager.

To create a configuration profile using Profile Manager:

1 Log in to your Mac OS X Server.

2 Open Services and find "Profile Manager" in the service list.

3 Click the **On** button to start the service.

4 In a Web browser, enter the URL for Profile Manager (e.g. `http://my_server.com/profilemanager/`).

5 Log in to Profile Manager using an administrator account.

6 In the Library, select the profile and click the **Edit** button to edit it. For a complete information about individual profile settings, see the documentation that comes with Profile Manager.

When setting up a Mac OS X profile for multiple users, it may not be possible to specify all of the settings in advance. For example, when confiuring the Exchange payload, the user account, email address, and password must be specified individually for each user. In a case like this, you may allow Mac users to provide the required settings interactively when the profile is applied on a Mac. The logic that determines whether the profile is applied on a Mac interactively or silently is as follows:

- To use the interactive mode, enter the `%user_interaction_required%` tag into a field instead of the actual value. If a payload contains this tag in at least one field, the Mac user will be prompted to manually enter all of the missing settings. The interactive mode will be used even if none of the missing settings are actually required on the Mac OS X side. You can enter the `%user_interaction_required%` tag into any field that you want a user to set manually.
- If a payload does not contain the `%user_interaction_required%` tag, an attempt will be made to apply the profile on a Mac silently. If the profile cannot be applied silently (one or more required settings are missing), the interactive mode will be used and the user will have to specify them manually.

In the interactive mode, a standard System Preferences dialog will be opened in Mac OS X for each corresponding payload where the user will have to specify the required settings. The dialog has the **Install** and **Cancel** buttons. To apply the settings, the user clicks the **Install** button. If the specified values are invalid, the user will have to enter them again. On success, a report will be sent to SCCM. If the user clicks the **Cancel** button, the profile installation is aborted and an appropriate report is sent to the administrator.

When you save the configuration profile, Profile Manager creates a file with the ".mobileconfig" extension. The file is an XML document containing the Mac OS X configuration settings that you specified. Copy the file to a location where the Configuration Manager console can access it (e.g. a directory on the server running the Configuration Manager console).

Enforcing FileVault 2 Encryption

FileVault 2 is an encryption method that can be used with volumes on Mac computers to keep their data secure. Parallels Mac Management for Microsoft SCCM 2012 provides a functionality to monitor and enforce FileVault 2 encryption on managed Macs.

Before creating a FileVault 2 configuration item, you need to decide whether you want to use an *institutional* or a *personal* recovery key. The following explains what these keys are.

When preparing to encrypt the disk, the Mac user is asked to specify a password that will be used to unlock an encrypted disk. If the user forgets the password, he/she will not be able to log into the computer. The *recovery key* is a "safety net" that can be used to unlock the disk if the user forgets the password.

When creating a FileVault 2 configuration item, you have an option to choose between the following key types:

- **Institutional**. An institutional recovery key is created in advance by the system administrator and then used for all Macs being encrypted. The key is stored in a keychain file, which the system administrator should keep in a safe place. If a Mac user forgets his or her personal password for unlocking the disk, this recovery key can be used to unlock it.

- **Personal**. A personal recovery key is created automatically for each individual Mac during the encryption procedure and is saved in the database on the primary SCCM site (p. 153). If a Mac user forgets the password for unlocking the disk, the personal recovery key for the disk can be retrieved from the database and can be used to unlock the disk.

Based on the type of the recovery key that you would like to use, read one of the following topics to learn how to create a FileVault 2 configuration item:

- **FileVault 2 Encryption with Institutional Recovery Key** (p. 67)
- **FileVault 2 Encryption with Personal Recovery Key** (p. 73)

FileVault 2 Encryption with Institutional Recovery Key

This section describes how to create a FileVault 2 configuration item using an institutional recovery key.

Creating FileVaultMaster Keychain

To use an institutional recovery key on multiple Macs, you need to create a FileVaultMaster keychain file. The file will contain a recovery key (private key) needed to recover a disk encrypted with FileVault 2 and a public certificate.

To create a FileVaultMaster keychain, run the following command in the Terminal (the command is available in Mac OS X 10.7.2 or later):

```
$ security create-filevaultmaster-keychain /path/to/FileVaultMaster.keychain
```

You can omit the target path and filename if you want to create the `FileVaultMaster.keychain` file in the default `/Users/`*`user-name`*`/Library/Keychains` directory.

When prompted, choose and enter a password for the new keychain, This will become your master password. After the keychain is created, make one or more backup copies of the `FileVaultMaster.keychain` file and store them in a safe location, such as an external drive or an encrypted volume.

You now need to export the X.509 asymmetric public certificate from the FileVaultMaster keychain to a DER encoded certificate file.

To export the certificate:

1. Run the Keychain Access application (Applications/Utilities).
2. In the **Keychain Access** window, select "FileVaultMaster" keychain in the **Keychains** panel.
3. In the right pane, right-click the "FileVault Recovery Key" certificate and then click **Export** in the pop-up menu.

4 Choose the name and location for the new file. Make sure that the **File Format** field has "Certificate (.cer)" option selected.

5 Click **Save** to export the certificate.

6 Copy the exported .cer file to a location where it can be accessed from the computer running the Configuration Manager 2012 console. You will later add this file to a configuration item to be distributed to Macs.

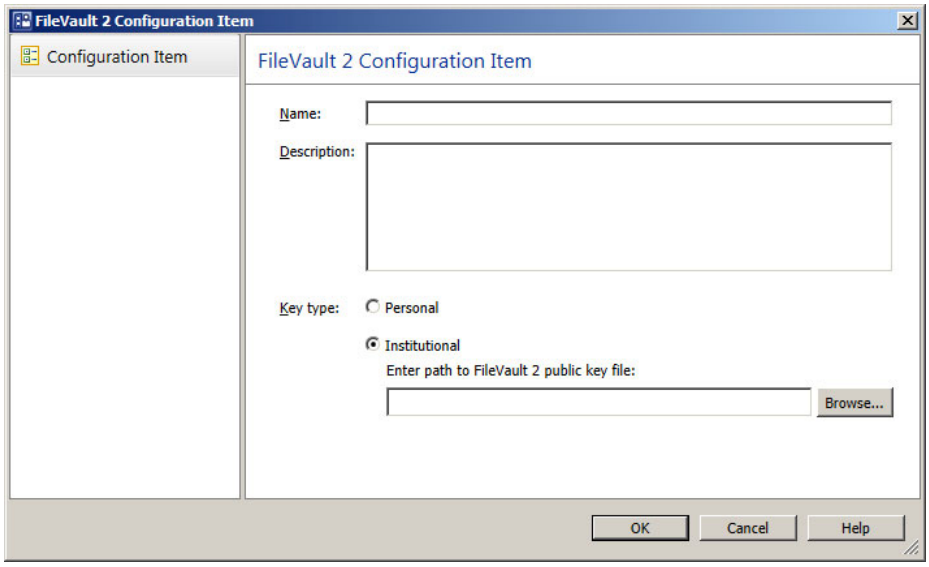
Creating FileVault 2 Configuration Item

To create a FileVault 2 configuration item using an institutional recovery key:

Note: If you want to use a personal recovery key, jump to **FileVault 2 Encryption with Personal Recovery Key** (p. 73).

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items** and then point to **Create Parallels Configuration Item** and click **FileVault 2 Configuration Item**.



3 Enter the desired configuration item name and description.

4 Select **Institutional** as key type. Please note that the following modifications are not allowed once the encryption has been performed on Mac computers:

- You cannot switch between personal and institutional key.
- You cannot change the existing FileVault 2 public key by providing another key file.

5 Click **OK** to create the configuration item.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

When a Mac is evaluated for compliance, an attempt will be made to enable FileVault 2 on it. The Mac user will be notified as follows:

1. A message box is displayed informing the user that the Mac is about to be encrypted. The dialog has two buttons: **Encrypt** and **Postpone**.
2. If the user clicks **Postpone**, the encryption operation will be postponed. The dialog will be displayed to the user again after a predefined period of time (five minutes). The user has the ability to keep postponing the encryption indefinitely. The time period after which the dialog is displayed again is doubled each time the user clicks **Postpone,** but never exceed one hour.
3. If the user clicks **Encrypt**, a window opens where the user must select one or more OS X user accounts that will be allowed to unlock the disk. To select an account, the user needs to click the **Enable** button next to the account name and then enter a password that will be used to unlock an encrypted disk. The user must enable at least one account to continue.
4. When the necessary accounts are selected, the user clicks **Encrypt** to enable FileVault 2. The user should then restart the Mac to encrypt the disk.

Viewing and Monitoring FileVault 2 Encryption Status

When the disk encryption operation is initiated on a Mac, the Parallels Mac Client begins reporting the encryption status to the Parallels Configuration Manager Proxy. The current encryption status is saved in the Mac's hardware inventory record in the Configuration Manager database and can be viewed in the Configuration Manager console. If at some later point the Mac user (or a third-party program) encrypts, decrypts, or re-encrypts the disk, the Parallels Mac Client running on a Mac will detect it and the database record will be immediately updated.

You can view the FileVault 2 encryption status for a particular Mac or you can run a report and view the information for all Macs in a single list.

Viewing the FileVault 2 Status for a Specific Mac

1. In the Configuration Manager console, open the collection containing your Mac resources (e.g. **All Mac OS X Systems**).
2. Locate the Mac of interest, right-click it and select **Start > Resource Explorer** from the pop-up menu. The **ResourceExplorer** snap-in opens.
3. In the resource tree, navigate to **Hardware** / **FileVault 2 Disk Encryption**. The encryption information for the Mac is displayed in the right pane.
4. A single row of information represents a corresponding Mac volume and contains the following columns:

- **Key Type** — the type of the recovery key that was assigned or created during encryption. The possible values are:
  - **Unknown** — the disk is not encrypted or the disk is encrypted by the Mac user or a third-party (see the **Status** column).
  - **Personal** — personal recovery key.

  - **Institutional** — institutional recovery key.
- **Status** — the current encryption status. The possible values are described in the table below.
- **Volume** — the volume name.

Viewing the FileVault 2 Disk Encryption Report

5 In the Configuration Manager console, navigate to **Monitoring** / **Reporting** / **Reports**.

6 Locate the **FileVault 2 Disk Encryption** report and double-click it. The **FileVault 2 Disk Encryption** dialog opens displaying the report.

7 Each row in the report represents a corresponding Mac volume and contains the following columns:

  - **Netbios Name** — the Mac netbios name.
  - **Volume** — the volume name.
  - **Status** — the FileVault 2 encryption status (see the table above).
  - **Key Type** — the recovery key type (Unknown, Personal, or Institutional).
  - **Time** — the date and time the record was last updated.

The following table lists all possible FileVault 2 encryption states and transitions:

State/Transition	Description
FileVault 2 is Off	FileVault 2 is not enabled on the Mac.
Encryption initiated, waiting for reboot	FileVault 2 encryption is in progress. The Mac is about to be rebooted to complete the encryption.
Encryption in progress	Encryption is in progress.
Encrypted	The Mac has been encrypted with FileVault 2.
Decrypting	Decryption is in progress.
Decrypting finished, waiting for reboot	Decryption finished. The Mac is about to be rebooted to complete the decryption.
Decrypted	The Mac has been decrypted.
Encrypting in progress by a 3rd party	An encryption operation has been initiated on the Mac by the user or a third-party program.
Encrypted by a 3rd party	The Mac has been encrypted by the user or a third-party program.
Decrypting (after 3rd party encrypting)	A decryption operation is in progress. The original encryption was performed by the Mac user or a third-party program. The decryption has also been initiated by the user or a third-party program.
Decrypting finished (after 3rd party encrypting), waiting for reboot	The Mac has been decrypted. The original encryption was performed by the Mac user or a third-party program. The decryption was also performed by the user or a third-party program. The Mac is about to be rebooted.

After the Macs have been encrypted, the best way for the system administrator to monitor the Mac encryption status is to configure the baseline containing the FileVault 2 configuration item to run as often as necessary (e.g. daily). If an unauthorized change have been made to the FileVault 2 encryption, the baseline run will fail and will report an error to Configuration Manager. The system administrator will be able to see it and check the hardware inventory record for a particular Mac.

Note: You should be aware of one scenario when the FileVault 2 encryption status may not be reported accurately in the Mac hardware inventory. This will happen when a Mac is removed from the Configuration Manager site, the Parallels Mac Client is uninstalled from it, and the Mac is then assigned to the site again. If the Mac was encrypted with FileVault 2 prior to removing it from the site, the encryption status will be reported as **Encrypted by a 3rd party**. To make the status to report accurately, you'll need to decrypt the disk and then encrypt it again.

Recovering Encrypted Disk Using Password

If a FileVault 2 encrypted disk becomes unbootable, and the Mac user knows his/her password (and is authorized to unlock the disk), use the following steps to unlock the disk:

1. Boot your Mac from the Recovery HD partition by holding down **Command –R**.
2. Use the following command to list the available Core Storage volumes:
   ```
   $ diskutil cs list
   ```
3. Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.
4. Use the following command to unlock the disk. Be sure to insert the UUID from the previous step:
   ```
   $ diskutil corestorage unlockVolume UUID -stdinpassphrase
   ```
5. When asked, enter the password of an account that's authorized to unlock the disk.
6. If successful, the drive will unlock and mount. You'll be able to back up the data using Disk Utility, or by using a command line tool such as ditto.
7. Once the disk is unlocked, you can decrypt it by executing the following command:
   ```
   $ diskutil corestorage revert UUID -stdinpassphrase
   ```
   Once the volume is decrypted, you'll have full access to your hard disk.

Recovering Encrypted Disk Using Institutional Key

A recovery may be needed if a FileVault 2 encrypted disk becomes unbootable and/or if a Mac user forgets their password.

To unlock an encrypted disk using an institutional recovery key, you need the original FileVaultMaster.keychain file that contains the recovery key. You must also know the master password that you've set when you created the file.

Finding the Correct FileVaultMaster.keychain File

If you have more than one FileVaultMaster.keychain file and you forgot which one is which, you can compare the SHA1 fingerprint of the certificate in the file to the fingerprint of the original certificate that Parallels Mac Management has saved in its database (p. 153). If you know exactly which file contains the correct recovery key, skip this and the following sub-sections and read the **Unlock the Disk Using the Institutional Recovery Key** sub-section that follows them.

To retrieve the SHA1 fingerprint of the original certificate that used during encryption:

1. In the Configuration Manager console, navigate to the device collection containing the Mac (e.g. **All Mac OS X Systems**).
2. Locate the Mac in the list. If you can't find the Mac, read the subsection that follows this one.
3. Right-click the Mac and then click **Properties**.
4. In the **Properties** dialog, click the **FileVault 2** tab to view the FileVault 2 encryption information for the Mac. The properties are:
   - **Hardware ID**. Contains the Mac hardware ID.
   - **Serial Number**. Contains the Mac serial number.
   - **Personal Key.** Contains the personal recovery key (will be blank if an institutional key was used).
   - **Institutional key**. Contains the SHA1 fingerprint of the institutional key certificate (will be blank if a personal key was used).
   - **LVGUUID**. The UUID of the logical volume group.
   - **LVUUID**. The UUID of the logical volume.
   - **PVUUID**. The UUID of the physical volume.
5. Compare the value of the **Institutional key** property to the fingerprint of the certificate in a FileVaultMaster.keychain file. The file that has the matching fingerprint contains the correct institutional recovery key.

If You Can't Find the Mac in Any of the Collections

If the Mac is no longer assigned to the Configuration Manager site (i.e. you can't find it in any of the device collections), you can still retrieve its FileVault 2 encryption info from the Parallels Mac Management database (p. 153). The FileVault 2 encryption records are never deleted even for the Macs that are no longer assigned to the site.

To retrieve the FileVault 2 encryption info for an unassigned Mac:

1. In the Configuration Manager console, navigate to **Assets and Compliance** / **Parallels Mac Management**.
2. Right-click **FileVault 2 Encryption Information** and then click **Properties**.

3 In the **FileVault 2 Encryption Information** dialog, enter the Mac's serial number of hardware ID. Click **Search**.

4 If the Mac was previously encrypted through Parallels Mac Management, a dialog will open containing the FileVault 2 encryption properties for this Mac.

5 Use the value of the **Institutional key** property to compare it to the SHA1 fingerprint of the certificate in a FileVaultMaster.keychain file.

Unlock the Disk Using the Institutional Recovery Key

Assuming that you have the correct FileVaultMaster.keychain file, do the following to unlock the encrypted disk:

1 Boot your Mac from the Recovery HD partition by holding down **Command –R**.

2 Connect an external drive containing the original `FileVaultMaster.keychain` file.

3 Run Terminal (Application/Utilities). If the keychain is stored in an encrypted disk image, use the following command to mount it:

```
$ hdiutil attach /path/to/diskImage
```

4 Use the following command to unlock the `FileVaultMaster.keychain` file:

```
$ security unlock-keychain /path/to/FileVaultMaster.keychain
```

5 Enter the Master Password to unlock the keychain. If the password is accepted, the command prompt will return.

6 Use the following command to list the available Core Storage volumes:

```
$ diskutil cs list
```

7 Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.

8 Use the following command to unlock the encrypted disk. Be sure to insert the UUID from the previous step and the correct path to the keychain file:

```
$ diskutil cs unlockVolume UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

9 When the command completes, the volume will be unlocked and mounted. You'll be able to back up data using Disk Utility, or by using a command line tool such as ditto.

If the command fails, it is possible that the disk was re-encrypted by the Mac user or a third-party program. You can compare the UUIDs of the volumes displayed by the `diskutil cs list` command to the **LVGUUID, LVUUID,** and **PVUUID** values on the **FileVault 2** tab of the Mac **Properties** dialog (see the **Retrieve Personal Recovery Key** subsection above). The values should match. If they don't, it means that the disk was re-encrypted, in which case the recovery key stored in the keychain file will not work.

10 Once the disk is unlocked, you can decrypt it by running the following command:

```
$ diskutil cs revert UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

FileVault 2 Encryption with Personal Recovery Key

This section describes how to create a FileVault 2 configuration item using a personal recovery key.

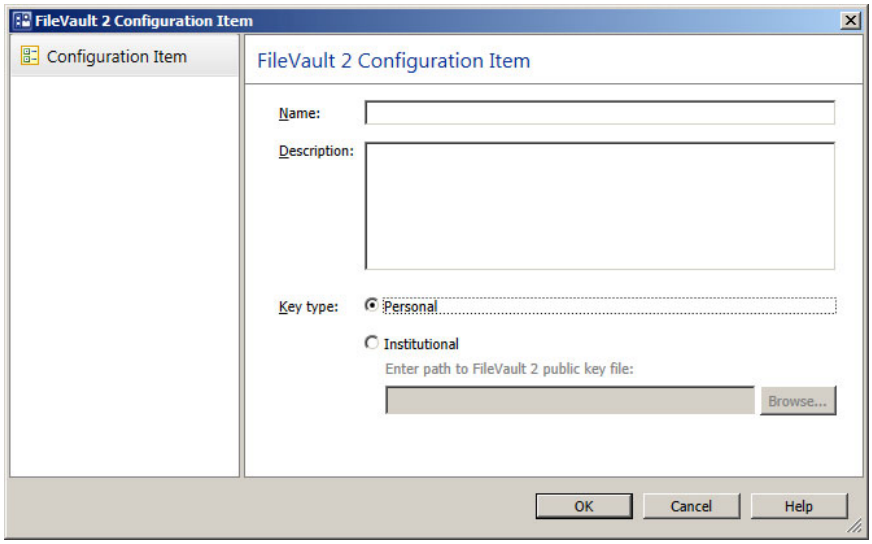
Creating FileVault 2 Configuration Item

To create a FileVault 2 configuration item using a personal recovery key:

Note: If you want to use an institutional recovery key, jump to **FileVault 2 Encryption with Institutional Recovery Key** (p. 67).

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items** and then point to **Create Parallels Configuration Item** and click **FileVault 2 Configuration Item**.



3 Enter the desired configuration item name and description.

4 Select **Personal** as key type. A personal recovery key will be created automatically for each Mac during the encryption operation. Each individual key will be stored in the database on the primary Configuration Manager site and can be retrieved and viewed in the Configuration Manager console.

Please note that you cannot switch between personal and institutional keys once the encryption has been performed on Mac computers:

5 Click **OK** to create the configuration item.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

When a Mac is evaluated for compliance, an attempt will be made to enable FileVault 2 on it. The Mac user will be notified as follows:

1 A message box is displayed informing the user that the Mac is about to be encrypted. The dialog has two buttons: **Encrypt** and **Postpone**.

2 If the user clicks **Postpone**, the encryption operation will be postponed. The dialog will be displayed to the user again after a predefined period of time (five minutes). The user has the ability to keep postponing the encryption indefinitely. The time period after which the dialog is displayed again is doubled each time the user clicks **Postpone,** but never exceed one hour.

3 If the user clicks **Encrypt**, a window opens where the user must select one or more OS X user accounts that will be allowed to unlock the disk. To select an account, the user needs to click the **Enable** button next to the account name and then enter a password that will be used to unlock an encrypted disk. The user must enable at least one account to continue.

4 When the necessary accounts are selected, the user clicks **Encrypt** to enable FileVault 2. The user should then restart the Mac to encrypt the disk.

Viewing and Monitoring FileVault 2 Encryption Status

When the disk encryption operation is initiated on a Mac, the Parallels Mac Client begins reporting the encryption status to the Parallels Configuration Manager Proxy. The current encryption status is saved in the Mac's hardware inventory record in the Configuration Manager database and can be viewed in the Configuration Manager console. If at some later point the Mac user (or a third-party program) encrypts, decrypts, or re-encrypts the disk, the Parallels Mac Client running on a Mac will detect it and the database record will be immediately updated.

You can view the FileVault 2 encryption status for a particular Mac or you can run a report and view the information for all Macs in a single list.

Viewing the FileVault 2 Status for a Specific Mac

1 In the Configuration Manager console, open the collection containing your Mac resources (e.g. **All Mac OS X Systems**).

2 Locate the Mac of interest, right-click it and select **Start > Resource Explorer** from the pop-up menu. The **ResourceExplorer** snap-in opens.

3 In the resource tree, navigate to **Hardware** / **FileVault 2 Disk Encryption**. The encryption information for the Mac is displayed in the right pane.

4 A single row of information represents a corresponding Mac volume and contains the following columns:

- **Key Type** — the type of the recovery key that was assigned or created during encryption. The possible values are:
  - **Unknown** — the disk is not encrypted or the disk is encrypted by the Mac user or a third-party (see the **Status** column).
  - **Personal** — personal recovery key.
  - **Institutional** — institutional recovery key.
- **Status** — the current encryption status. The possible values are described in the table below.
- **Volume** — the volume name.

Viewing the FileVault 2 Disk Encryption Report

5 In the Configuration Manager console, navigate to **Monitoring** / **Reporting** / **Reports**.

6 Locate the **FileVault 2 Disk Encryption** report and double-click it. The **FileVault 2 Disk Encryption** dialog opens displaying the report.

7 Each row in the report represents a corresponding Mac volume and contains the following columns:

- **Netbios Name** — the Mac netbios name.
- **Volume** — the volume name.
- **Status** — the FileVault 2 encryption status (see the table above).
- **Key Type** — the recovery key type (Unknown, Personal, or Institutional).
- **Time** — the date and time the record was last updated.

The following table lists all possible FileVault 2 encryption states and transitions:

State/Transition	Description
FileVault 2 is Off	FileVault 2 is not enabled on the Mac.
Encryption initiated, waiting for reboot	FileVault 2 encryption is in progress. The Mac is about to be rebooted to complete the encryption.
Encryption in progress	Encryption is in progress.
Encrypted	The Mac has been encrypted with FileVault 2.
Decrypting	Decryption is in progress.
Decrypting finished, waiting for reboot	Decryption finished. The Mac is about to be rebooted to complete the decryption.
Decrypted	The Mac has been decrypted.
Encrypting in progress by a 3rd party	An encryption operation has been initiated on the Mac by the user or a third-party program.
Encrypted by a 3rd party	The Mac has been encrypted by the user or a third-party program.
Decrypting (after 3rd party encrypting)	A decryption operation is in progress. The original encryption was performed by the Mac user or a third-party program. The decryption has also been initiated by the user or a third-party program.
Decrypting finished (after 3rd party encrypting), waiting for reboot	The Mac has been decrypted. The original encryption was performed by the Mac user or a third-party program. The decryption was also performed by the user or a third-party program. The Mac is about to be rebooted.

After the Macs have been encrypted, the best way for the system administrator to monitor the Mac encryption status is to configure the baseline containing the FileVault 2 configuration item to run as often as necessary (e.g. daily). If an unauthorized change have been made to the FileVault 2 encryption, the baseline run will fail and will report an error to Configuration Manager. The system administrator will be able to see it and check the hardware inventory record for a particular Mac.

Note: You should be aware of one scenario when the FileVault 2 encryption status may not be reported accurately in the Mac hardware inventory. This will happen when a Mac is removed from the Configuration Manager site, the Parallels Mac Client is uninstalled from it, and the Mac is then assigned to the site again. If the Mac was encrypted with FileVault 2 prior to removing it from the site, the encryption status will be reported as **Encrypted by a 3rd party**. To make the status to report accurately, you'll need to decrypt the disk and then encrypt it again.

Recovering Encrypted Disk Using Password

If a FileVault 2 encrypted disk becomes unbootable, and the Mac user knows his/her password (and is authorized to unlock the disk), use the following steps to unlock the disk:

1. Boot your Mac from the Recovery HD partition by holding down **Command –R**.
2. Use the following command to list the available Core Storage volumes:
   ```
   $ diskutil cs list
   ```
3. Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.
4. Use the following command to unlock the disk. Be sure to insert the UUID from the previous step:
   ```
   $ diskutil corestorage unlockVolume UUID -stdinpassphrase
   ```
5. When asked, enter the password of an account that's authorized to unlock the disk.
6. If successful, the drive will unlock and mount. You'll be able to back up the data using Disk Utility, or by using a command line tool such as ditto.
7. Once the disk is unlocked, you can decrypt it by executing the following command:
   ```
   $ diskutil corestorage revert UUID -stdinpassphrase
   ```
   Once the volume is decrypted, you'll have full access to your hard disk.

Recovering Encrypted Disk Using Personal Key

A recovery may be needed if a FileVault 2 encrypted disk becomes unbootable and/or if a Mac user forgets their password. In such a case, a recovery key must be used to unlock the disk.

To unlock or decrypt an encrypted disk using this option you will need the personal recovery key that was created when the Mac was encrypted.

Retrieve Personal Recovery Key

First, you need to retrieve the personal recovery key for a Mac that you want to recover. The key is stored in the Parallels Mac Management database (p. 153) and can be obtained as follows:

1. In the Configuration Manager console, navigate to the device collection containing the Mac (e.g. **All Mac OS X Systems**).
2. Locate the Mac in the list. If you can't find the Mac, read the subsection that follows this one.
3. Right-click the Mac and then click **Properties**.

4 In the **Properties** dialog, click the **FileVault 2** tab to view the FileVault 2 encryption information for the Mac. The properties are:

- **Hardware ID**. Contains the Mac hardware ID.
- **Serial Number**. Contains the Mac serial number.
- **Personal Key.** Contains the personal recovery key (will be blank if an institutional key was used).
- **Institutional key**. Contains the SHA1 fingerprint of the institutional key certificate (will be blank if a personal key was used).
- **LVGUUID**. The UUID of the logical volume group.
- **LVUUID**. The UUID of the logical volume.
- **PVUUID**. The UUID of the physical volume.

5 Copy the value of the **Personal key** property. If the property doesn't have a value but the **Institutional key** property underneath it does, then this Mac was encrypted with an institutional key. For institutional key instructions, please read **Recovering Encrypted Disk Using Institutional Key** (p. 71).

If You Can't Find the Mac in Any of the Collections

If the Mac is no longer assigned to the Configuration Manager site (i.e. you can't find it in any of the device collections), you can still retrieve the personal recovery key for it from the Parallels Mac Management database (p. 153). The FileVault 2 encryption records are never deleted from it even for the Macs that are no longer assigned to the site.

To retrieve the personal key for an unassigned Mac:

1 In the Configuration Manager console, navigate to **Assets and Compliance** / **Parallels Mac Management**.

2 Right-click **FileVault 2 Encryption Information** and then click **Properties**.

3 In the **FileVault 2 Encryption Information** dialog, enter the Mac's serial number of hardware ID. Click **Search**.

4 If the Mac was previously encrypted, a dialog will open containing the FileVault 2 encryption properties for this Mac.

5 Copy the value of the **Personal key** property.

Unlock the Disk Using the Personal Recovery Key

Once you have the personal recovery key, you can use it to unlock the encrypted disk:

1 Boot your Mac from the Recovery HD partition by holding down **Command –R**.

2 Use the following command to list the available Core Storage volumes:

```
$ diskutil cs list
```

3 Look for the UUID of a Logical Volume, usually the last in the list. Select and copy the UUID to be used in the next step.

4 Use the following command to unlock the encrypted disk. Be sure to insert the UUID from the previous step:

```
$ diskutil cs unlockVolume UUID -passphrase recoverykey
```

5 When the command completes, the volume will be unlocked and mounted. You'll be able to back up data using Disk Utility, or by using a command line tool such as ditto.

If the command fails, it is possible that the disk was re-encrypted by the Mac user or a third-party program. You can compare the UUIDs of the volumes displayed by the `diskutil cs list` command to the **LVGUUID, LVUUID,** and **PVUUID** values on the **FileVault 2** tab of the Mac **Properties** dialog (see the **Retrieve Personal Recovery Key** subsection above). The values should match. If they don't, it means that the disk was re-encrypted, in which case the recovery key stored in the Parallels Mac Management database will not work.

6 Once the disk is unlocked, you can decrypt it by running the following command:

```
$ diskutil cs decryptVolume UUID -passphrase recoverykey
```

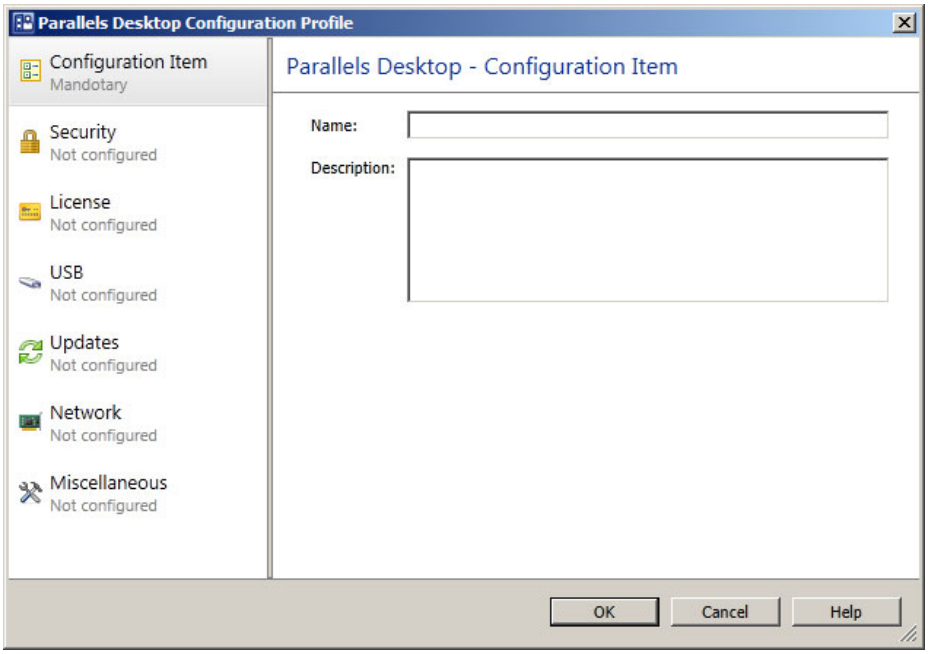
Enforcing Parallels Desktop Preferences

If you have Parallels Desktop running on your Macs, you can monitor and enforce its preferences by creating a Parallels Desktop configuration item and specifying the required values.

To create a Parallels Desktop configuration item:

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.

2 Right-click **Configuration Items**, point to **Create Parallels Configuration Item** and click **Parallels Desktop Configuration**. The **Parallels Desktop Configuration Profile** dialog opens.



The following list describes the organization of the **Parallels Desktop Configuration Profile** dialog:

- **Configuration Item**. Specifies the name and description of the configuration profile.
- **Security**. Specifies whether a password is required to create, add, remove, and clone virtual machines. If an option is selected here, a Mac user will have to enter a password to use it in Parallels Desktop. Also specifies whether a user is allowed to change Parallels Desktop preferences. To enable password requirements, click the ON/OFF switch to toggle it to "ON" and then select the desired options.
- **License**. Used to specify the Parallels Desktop license key and customize the Request Support options. You can specify the license key when you want to update the license on managed Macs. The Request Support options define what happens when a Mac user clicks the **Help** > **Request Support** menu item in the Parallels Desktop graphical user interface.
- **USB**. Specifies the USB behavior.
- **Updates**. Specifies the Parallels Desktop automatic update options.
- **Network**. Specifies the Parallels Desktop network settings.
- **Miscellaneous**. Specifies the default virtual machine folder and whether or not the users should participate in the Parallels Customer Experience program.

When finished, click **OK** to save the profile and close the dialog. To modify the profile, right-click it and then click **Edit Parallels Configuration Item** in the pop-up menu.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

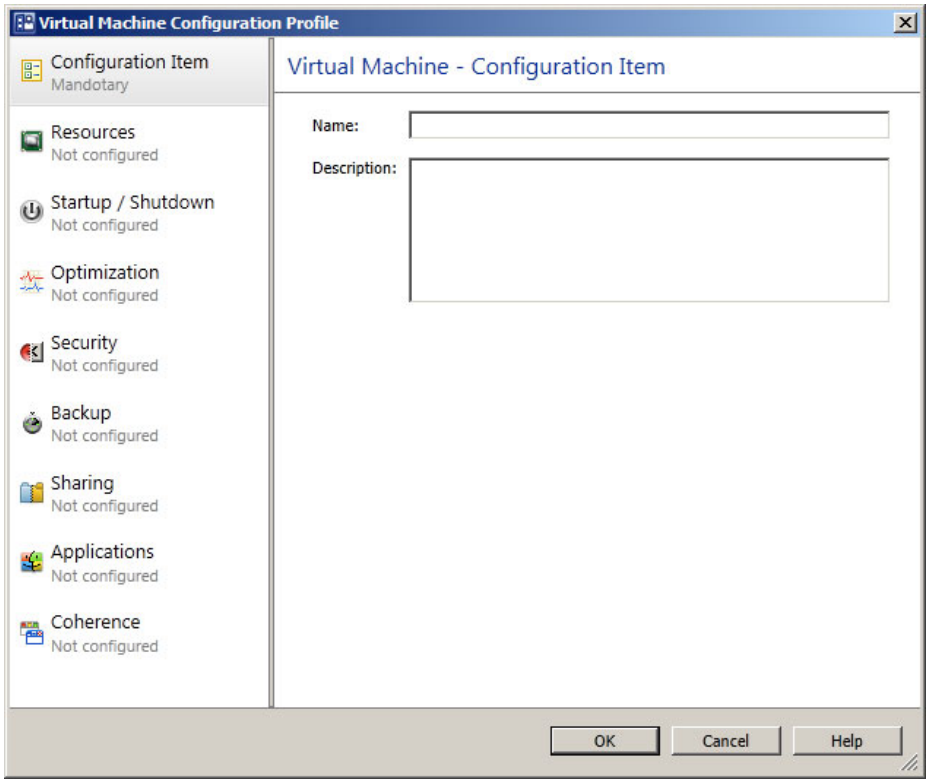
Enforcing Parallels Desktop VM Settings

A Parallels Desktop virtual machine has numerous configuration options that can be customized on client Macs according to your organization requirements. To monitor Macs for virtual machine configuration compliance you need to create a virtual machine configuration item specifying the desired configuration parameters.

Note: The settings that you specify in a virtual machine configuration item will be applied to all existing virtual machines on a given Mac.

To create a virtual machine configuration item:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Items**, point to **Create Parallels Configuration Item** and click **Parallels Virtual Machine Configuration**. The **Virtual Machine Configuration Profile** dialog opens.



3. To specify the virtual machine configuration options to monitor, select an item in the left pane and specify individual configuration settings in the right pane.

4 To include an option in the configuration profile and to specify its value click the ON/OFF switch to toggle it to "ON". To exclude an option, toggle the switch to "OFF". The excluded options will not be evaluated on managed Macs.

5 When finished, click the **OK** button to close the dialog. To modify the profile, right-click it and then click **Edit Parallels Configuration Item** in the pop-up menu.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

Using Scripts to Assess Compliance

In addition to configuration profiles described in the previous sections, you can assess the configuration compliance of client Macs using scripts written in any language supported by OS X.

To use scripts, you need to create a standard SCCM configuration item in the Configuration Manager console. When creating a configuration item, you have an option to specify a *discovery script* and a *remediation script*. The discovery script is used to obtain the value of a setting on a Mac to be assessed for compliance. The remediation script is used to remediate a noncompliant value if needed (creating a remediation script is optional).

When a discovery script returns a value, it is assessed for compliance using the *compliance rules* defined for it. If the value is noncompliant and a remediation script exists, the value is passed to the script so that the necessary modifications can be done on the Mac. If a remediation script doesn't exist, the assessment stops and a noncompliance is reported to SCCM. Each discovery script can assess a single value, but multiple scripts with their own compliance rules can be added to a given configuration item.

This section describes how to:

- Create a configuration item using the **Create Configuration Item Wizard** (p. 82)
- Create a discovery script (p. 84)
- Create a remediation script (p. 84)
- Specify the script interpreter to be used (p. 85)
- Define Compliance Rules (p. 85)

Creating Configuration Item

To use scripts to assess compliance, you need to create a standard SCCM configuration item. To do so, in the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**. Right-click **Configuration Items** and then click **Create Configuration Item** in the pop-up menu. The **Create Configuration Item Wizard** opens. Populate the pages of the wizard as described below.

General Page

Specify the general properties of the configuration item:

1. Specify the configuration item **Name** and an optional **Description**.
2. Select **Mac OS X** in the **Specify the type of configuration item that you want to create** list box.
3. Click **Next**.

Supported Platforms Page

Select the OS X versions to which this configuration item should be applicable. Please note that this selection will be ignored in the future releases of Parallels Mac Management. If at that time you'll need to exclude a particular OS X version, you can create multiple Mac collections based on the OS X version criteria and then selectively deploy the configuration item to them.

Settings Page

The **Settings** page is used to create a set of *settings* representing the conditions to assess for compliance on Mac computers. In our case, each *setting* will evaluate a particular value on a Mac.

To create a new setting:

1. Click **New** to open the **Create Setting** dialog.
2. In the **Create Setting** dialog, specify the setting **Name** and an optional **Description**.
3. In the **Setting type** list box, select **Script**.
4. In the **Data type** list box, select the data type of the value that this setting will evaluate on a Mac. The discovery script that you'll specify later should return a value of the same data type in the string format.
5. In the **Discovery script** section, click **Add Script**. The **Edit Discovery Script** dialog opens where you can specify the discovery script. See **Creating Discovery Script** (p. 84) for the complete information.
6. If you would like to create a remediation script, click **Add Script** in the **Remediation script** section. The **Create Remediation Script** dialog opens where you can specify the remediation script. See **Creating Remediation Script** (p. 84) for the complete information.
7. Once you've specified the discovery and remediation scripts, you need to define compliance rules specifying the conditions that make the value returned by the discovery script compliant on Macs. To define compliance rules, make sure that you are back in the **Create Setting** dialog and click the **Compliance Rules** tab. To create a new rule, click **New** to open the **Create Rule** dialog. Use the dialog to define the rule. See **Defining Compliance Rules** (p. 85) for the complete information. You can create more than one rule for a given configuration item setting.
8. When you are finished specifying scripts and compliance rules, click **OK** in the **Create Setting** dialog and then click **Next** on the **Settings** page of the wizard.

Compliance Rules Page

The **Compliance Rules** page lists the compliance rules that you've created earlier. You can review and modify them if necessary. You can also create new rules here if needed. Click **Next** when ready.

Summary, Progress, and Completion Pages

Review the configuration item summary and click **Next** when ready. Wait for the configuration item to be created. Review the info on the **Completion** page and click **Close** to exit the wizard.

To evaluate Mac computers for compliance, you need to add the configuration item to a baseline and then deploy it to a Mac collection. See **Deploying Configuration Baseline** (p. 86) for more information.

Creating Discovery Script

A discovery script is specified using the **Edit Discovery Script** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 82).

The script can be written in any scripting language supported by OS X, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 85) for additional information.

You can type (or copy and paste) the script into the **Script** edit box. If you have the script saved in a file, click the **Open** button to browse for it.

A discovery script is used to find and return a value to be assessed for compliance on a Mac. The value can be of any data type supported by Configuration Manager, but must be returned by the discovery script as a string. Write the script to obtain the value of a desired setting on a Mac and return it as a string via standard output. The returned value is evaluated using the compliance rules defined for this configuration item setting. If the value is noncompliant and a remediation script exists (p. 84), the value will be passed to the remediation script for evaluation. If the remediation script doesn't exist, the assessment stops and noncompliance is reported to SCCM.

Please note that a discovery script will run in OS X with root privileges. Please also note that you cannot access OS X GUI components from a discovery script. For example, you cannot open a dialog to be displayed to the Mac user.

Creating Remediation Script

A remediation script is created using the **Create Remediation Script** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 82).

The script can be written in any scripting language supported by OS X, such as Bash, Python, Apple Script, etc. See **Specifying Script Interpreter** (p. 85) for additional information.

You can type (or copy and paste) the script into the **Script** edit box. If you have the script saved in a file, click the **Open** button to browse for it.

A remediation script is used to remediate noncompliant setting values found on a Mac. The noncompliant value is passed to the script as an input parameter after obtaining it with the discovery script and assessing it using the compliance rules. A remediation script should return 0 (zero) as a string via standard output.

When the remediation script returns, the discovery script is executed again to obtain the updated value. The value is then evaluated using the compliance rules. If the value complies, the assessment finishes with success. If the value is still noncompliant, a noncompliance is reported to SCCM.

Please note that a remediation script will run in OS X with root privileges. Please also note that you cannot access OS X GUI components from a remediation script. For example, you cannot open a dialog to be displayed to the Mac user.

Specifying Script Interpreter

When creating a discovery or a remediation script, use the syntax described below to specify the interpreter that should be used to run it.

The first line of the script should begin with shebang and have the following format:

#! *interpreter* [*interpreter-args*] *<args-list-terminator>* [**#***comment*]

where:

- *interpreter* is the absolute path to the interpreter executable (e.g. `/bin/bash`).
- *interpreter-args* is the list of the interpreter arguments.
- *args-list-terminator* is the terminating character of the argument list. The terminator is needed for passing the result of the discovery script to the remediation script.

  Python example:

  ```
  #! /usr/bin/python -
  ```

  Bash example:

  ```
  #! /bin/bash --
  ```
- *comment* is a comment that you might want to add to the script.

Creating Compliance Rules

A compliance rule defines compliance conditions for the value returned by the discovery script. The conditions are defined using the **Create Rule** dialog, which is opened from the **Create Setting** dialog, which in turn is opened from the **Create Configuration Item Wizard** (p. 82).

To create a rule, do the following in the **Create Rule** dialog:

1. Specify the rule **Name** and an optional **Description**.
2. Set the **Rule type** to **Value**.
3. Use the **The setting must comply with the following rule** section to specify the rule.
4. If you specified a remediation script for this configuration item setting, you may select the **Run the specified remediation script when this setting is noncompliant** option. If this option is selected and the value is noncompliant, the remediation script will be executed and the value will be passed to it as a parameter.
5. The **Report noncompliance if this setting instance is not found** option affects the compliance or non-compliance reporting. When the script execution doesn't fail, but doesn't return any data either, the rule is not evaluated. Instead, the compliance status is determined by the state of this option as follows:
   - If the option is selected, compliance is reported.
   - If the option is cleared, non-compliance is reported.
6. Click **OK** to create the rule and close the dialog.

You can create more than one rule for a given configuration item setting. If there's more than one rule, they will be connected using the logical AND operator. Therefore, for a value to be compliant, all rules must evaluate as TRUE.

Deploying Configuration Baseline

Once you've created one or more configuration items, you need to add them to a configuration baseline. Configuration baseline is a container that combines configuration items into a logical unit so they can be evaluated for compliance by Macs as a group. You can add configuration items to an existing baseline or you can create a new one.

To create a configuration baseline:

1. In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Compliance Settings**.
2. Right-click **Configuration Baselines** and then click **Create Configuration Baseline** in the pop-up menu. The **Create Configuration Baseline** dialog opens.
3. Enter the desired configuration baseline name and description.
4. Click the **Add** button and then select the configuration items that you want to add to the baseline. Click **OK** and click **OK** again.

The new configuration baseline will appear in the **Configuration Baselines** list. You can click **Refresh** on the toolbar to refresh the list.

Once a configuration baseline is created, you need to deploy it to a Mac collection.

To deploy a configuration baseline:

1. In the Configuration Manager console, right-click the baseline that you've created and click **Deploy** in the pop-up menu.
2. In the **Deploy Configuration Baselines** dialog, click the **Browse** button.
3. In the **Select Collection** dialog, select **Device Collections** in the drop-down list box and then select the **All Mac OS X Systems** collection in the list. Click **OK**.
4. When back in the **Deploy Configuration Baselines** dialog, specify the desired schedule for the baseline and click **OK**.

A configuration baseline will run as scheduled for as long as it exists. To delete a baseline, right-click it and then click **Delete**.

Receiving DCM Reports

Corporate policies can be enforced on Mac OS X computers using the Desired Configuration Management. Parallels Mac Management for Microsoft SCCM provides a reporting functionality that allows to evaluate the results of enforcing corporate policies on individual Mac computers.

To enforce a policy, the IT administrator creates a configuration item, adds it to a baseline, and then deploys the baseline to a Mac collection. When the baseline runs, each configuration item is applied to a Mac and modifies a corresponding configuration according to the rules that it contains.

After the configuration changes are made to the Mac, the following reports are generated on the Mac side:

- A report for each configuration item applied to a Mac (a configuration baseline can contain more than one configuration item, so a report is generated for each individual item).
- A summary report for the baseline after all configuration items are applied to a Mac.

As soon as a report is generated, the Mac Client sends it to the Configuration Manager Proxy, which sends it to the Configuration Manager. When the Mac evaluation for compliance completes, the IT administrator can view the reports in the Configuration Manager console. If the client software on the Mac cannot establish a connection with the Configuration Manager Proxy, the reports are saved locally on the Mac and the transfer is resumed as soon as the connection becomes available.

To view the DCM evaluation reports in the Configuration Manager console, you need a Reporting Point set up on your Configuration Manager site. If you don't have a Reporting Point, set it up in the Configuration Manager console using the standard Configuration Manager functionality.

To view the Desired Configuration Management reports:

1. In the Configuration Manager console, navigate to **Site Database** / **Computer Management** / **Reporting** / **Reports**.
2. In the report list, find the "Compliance for a computer by configuration item" report or the "Compliance for a computer by configuration baseline" report, right-click it and then click **Run** in the pop-up menu.

3 Specify the report criteria using the provided options (computer name, configuration item name).

4 Click **Display** to view the report.

A compliance report contains the basic information about the Mac computer and the configuration item (or configuration baseline) together with the following items describing the results of the Mac compliance evaluation:

- **Compliance State** — describes whether the Mac complies with the corporate policies defined in the configuration item(s). The possible values are Compliant and Non-compliant.
- **Last Evaluation Date and Time (UTC)** — contains the last evaluation date and time.

Application Management

Application management in System Center 2012 Configuration Manager provides the tools to manage applications in the enterprise. Applications are similar to distribution packages, but contain more information to support smart deployment. Parallels Mac Management natively supports the application management feature of System Center 2012 Configuration Manager and allows to use it to deploy applications on Mac computers.

The steps to create and deploy a Mac application are:

1 Decide whether you want the application to be installed on a Mac silently or interactively (p. 88)

2 Prepare a Mac application for Configuration Manager (p. 89)

3 Create a Configuration Manager application for the Mac software (p. 89)

4 Configure the Deployment Type (p. 91)

5 Deploy the Mac application (p. 93)

The remaining topics in this section describe how the application is installed on a Mac and how to use Application Portal:

- Installing Application on a Mac (p. 95)
- Using Application Portal (p. 96)

Choosing Installation Type

When preparing a Mac application for deployment, you can configure it to be installed on a Mac silently or with user interaction.

Silent Installation

If you configure the application to install silently, it will be delivered to a Mac and installed without giving the user any control over the installation process. The only operation that the user will be asked to confirm is restarting the Mac if it is required by a particular application. The options that must be set in order to perform a silent installation are highlighted in the corresponding topics describing the application deployment steps.

Interactive Installation

An interactive installation informs the Mac user that the application is available for installation and, depending on the deployment configuration, gives the user full or limited control over the installation process.

When preparing an application for interactive installation, you can specify the following options:

- An application can be either required to be installed or the user can be given a choice whether to install it or not.
- The application installer can be displayed on the screen allowing the user to control the installation process, or the installer can run in the background thus performing an unattended installation. In both scenarios the user can choose whether to run the installer as soon as the application is available or to postpone it to a later time.

The options that must be set in order to perform an interactive installation are highlighted in the corresponding topics describing the application deployment steps.

Application Portal

When an application is configured to be deployed interactively as described above, it will be added to Application Portal on a Mac. Application Portal is an OS X application (provided by Parallels) that allows a Mac user to view and install applications made available to them by their system administrator. Application Portal is installed when the Parallels Mac Client is installed on a Mac.

When preparing an application for deployment, you need to specify the properties that will be used in Application Portal to provide a Mac user the ability to identify, filter, and sort the available applications. The properties that relate to Application Portal are highlighted in the corresponding topics describing the application deployment steps. Application Portal is described in detail in the **Using Application Portal** section (p. 96).

Preparing Mac Application for Configuration Manager

Before you can deploy OS X application packages to Mac computers, you must use the **CMAppUtil** utility to convert them to a Configuration Manager **.cmmac** format.

The **CMAppUtil** utility is provided by Microsoft. To obtain the utility:

1. Download the **ConfigmgrMacClient.msi** file from the Microsoft Download Center. Use one of the following URLs depending on the SCCM version you are using:
   - SCCM 2012 R2: http://www.microsoft.com/en-us/download/details.aspx?id=39360
   - SCCM 2012: http://www.microsoft.com/en-us/download/details.aspx?id=36212
2. Run the file on your Windows computer to extract the **macclient.dmg** file. The file is extracted by default to "C:\Program Files\Microsoft (x86)\System Center 2012 Configuration Manager Mac Client".
3. Copy the **macclient.dmg** file to a Mac computer.
4. Double-click the file to see its contents. Extract the **Tools** folder from the file by dragging and dropping it to a folder on your Mac hard drive (e.g. the same folder as the **macclient.dmg** file).

To convert an OS X disk image file to the **.cmmac** format:

1. Copy the disk image file (.dmg) that you want to deploy to Mac computers to the folder where you extracted to **Tools** folder.
2. Navigate to the **Tools** folder and enter the following command-line:

   ./CMAppUtil *<properties>*

   For example, to convert an Apple disk image file named **MySoftware.dmg** stored in the user's home folder to the **.cmmac** format:

   ./CMApputil –c /Users/ *<User Name>* **/MySoftware.dmg -o /Users/** *<User Name>*

   The command above creates a **.cmmac** installation file compatible with Configuration Manager. The **-c** option specifies the source file being converted. The **-o** option specifies the output path. For the complete list of options, please consult the Microsoft **CMAppUtil** documentation.

When you have the **.cmmac** file, copy it to a network share where it can be accessed from the computer running the Configuration Manager console.

Creating Configuration Manager Application

To create a Configuration Manager application using the **Create Application Wizard**:

1. In the Configuration Manager Console, navigate to **Software Library** / **Application Management**.
2. Right-click **Applications** and click **Create Application**. This will open the **Create Application Wizard**.
3. Populate the **Create Application Wizard** pages as follows.
4. On the **General** page, in the **Type** drop-down list, select **Mac OS X**.
5. Click **Browse,** enter the network location of the `.cmmac` file that you've prepared earlier, select the file and click **Open**.
6. Click **Next**. Review the information on the **Import Information** page and click **Next**.

7 On the **General Information** page, specify the application name, and optionally publisher, and version. Click **Next**.

8 Review the application settings on the **Summary** page and click **Next**.

9 Wait until the application is created and then click **Close** to close the wizard.

The new application will appear in the **Applications** list in the Configuration Manager console**.**

Specify Application Properties for Application Portal

The application properties described here determine how the application will be displayed in Application Portal on a Mac and will be used as filter criteria. If you would like to configure the application to be installed silently without adding to Application Portal (you will choose the installation type later), you may skip this sub-section.

To set the application properties for Application Portal:

1 Right-click the application that you've created in the previous step and click **Properties** in the context menu. This will open the <*application_name*> **Properties** dialog.

2 Click the **Application Catalog** tab and set the following properties:

- **Selected language** — Select the language version of the application from the drop-down list. Click **Add/Remove** to add additional languages if needed.
- **Localized application name —** Specify the application name in the language selected in the **Selected language** field.
- **User categories —** Click **Edit** to specify user categories that the users of the catalog can use to filter and sort the available applications.
- **Icon —** Click **Browse** to select an icon for this application.
- **Display this as a featured app and highlight it in the company portal —** If you select this option, the application will be listed in the **Featured Applications** list in Application Portal on a Mac. The list is displayed on the **All Applications** tab page in Application Portal and is immediately visible to the user.

3 If the application that you are creating is an upgrade or a replacement for an existing application in Application Portal, then you can specify a supersedence relationship on the **Supersedence** tab page. Select the **Allow users to see deployments for this an all applications that it supersedes**... option if you want to display all versions iof the application n Application Portal. If the option is cleared, only the top application will be shown in Application Portal.

4 Click **OK** to close the **Properties** dialog.

Configuring Deployment Type

A deployment type for the application is created automatically when you create the Configuration Manager application. This section describes some of the deployment type properties that you may want to modify.

To modify the properties of the deployment type:

1 Select the **Deployment Types** tab at the bottom of the **Applications** workspace.

2 Right-click the deployment type and click **Properties** in the context menu.

3 The <*application_name*> **- Mac OS X Properties** dialog opens.

Use the following instructions to modify the deployment type properties as needed.

Specify the Installation Command Line

To specify the command that you want to use to install, and optionally uninstall, the application on a Mac, click the **Programs** tab. The **Installation program** field is used to specify the command line. The field is populated automatically and should already contain the installation command for the application. You can modify the command line as needed.

If you've configured the application for Application Portal, you can optionally specify an uninstallation command for it. This will enable the **Remove** button in Application Portal and will provide a convenient method for removing an application from a Mac. To add the uninstallation command line, use the following syntax:

:<*Installation command*>**:**<*Uninstallation command*>**:**

The <*Installation command*> and <*Uninstallation command*> parts should contain the installation and uninstallation commands respectively. You have to find out what the actual uninstallation command line for a given application is yourself.

As an example, the following command line contains the installation and uninstallation commands for Firefox (please note the colon characters, which are required):

:/usr/bin/ditto "Firefox.app" "/Applications/Firefox.app":rm -rf "/Applications/Firefox.app":

When you add the uninstallation command to the command line, the **Remove** button in Application Portal becomes available once the application is installed on a Mac. If you don't include an uninstallation command, the **Remove** button in Application Portal will not be available for the given application.

Specify the Mandatory Mac Restart Option

To force a mandatory Mac restart after the application is installed on it:

1 Click the **User Experience** tab.

2 In the **Action** drop-down list, select the action from the following options:

- **No action** — The Mac will be restarted only if the application installer requires it.
- **Configuration Manager client will force a mandatory device restart** — The Mac will be restarted regardless of whether the application installer requires it or not.

Specify Detection Method

The **Detection Method** tab page allows to specify how Configuration Manager determines whether this deployment type is already present on a Mac. This information is automatically imported when you convert the OS X installation image to a **.cmmac** file.You can modify the imported information, if needed, by editing the existing clause or creating a new one.

To modify or create a clause:

3 On the **Detection Method** tab page, select the existing clause and click **Edit Clause** (or click **Add Clause**).

4 Select the **Setting Type**. The available options are **Application Bundle** and Package **ID:**

- For **Application Bundle**, specify **Application bundle ID**, **Data Type** (**String** or **Version**), **Operator,** and **Value**.
- For **Package ID**, specify **Package ID**, **Operator**, and **Value**.

5 Click **OK** to save the changes and close the dialog.

Specify System Requirements

The **Requirements** tab page allows you to specify system requirements that must be met to allow the application to be installed. The only requirement that can be currently specified is the OS X version.

To specify the OS X version requirement:

1 On the **Requirements** tab page, click the **Add** button.

2 In the **Category** drop-down list, select **Device**.

3 In the **Condition** list, select **Operating system**.

4 In the OS X tree, select one or more OS X versions. If you check **Select all**, all existing and all future OS X versions will satisfy the requirement.

5 Click **OK** to save the changes and close the dialog.

Deploying Mac Application

After you've created the Configuration Manager application and configured the deployment type, you need to deploy the application to a Mac collection.

To deploy the application:

1 Right-click the application and click **Deploy** in the context menu. This will open the **Deploy Software Wizard**.

2 On the **General** page, click **Browse** to select the target Mac collection.

3 In the **Select Collection** dialog, select **Device Collection** in the drop-down list, and then select the target collection (e.g. **All Mac OS X Systems**). Click **OK**.

4 Click **Next**.

5 On the **Content** page, click **Add** to add a Distribution Point that will host this content. Select a Distribution Point and click **OK**.

6 Click **Next**.

7 On the **Deployment Settings** page, in the **Action** drop-down list, select **Install**.

8 In the **Purpose** list, select **Available** or **Required:**

- If you select **Available**, the Mac user will be informed that the application is available for installation, but will not be required to install it.
- If you select **Required**, the user will be required to install the application. If you want the application to be installed silently, you must select this option and also select the **Hide in Software Center and all notifications** option described in step 12 below.

9 Click **Next**.

10 On the **Scheduling** page, specify the schedule at which this application should be available to Mac users.

If you've selected the application **Purpose** as **Required** on the previous page (step 8 above), you'll need to specify the **Installation deadline** for the application. The following deadline options are available:

- **As soon as possible** — Mac users will be required to install the application as soon as it is available. If a user fails to install the application right away, he/she will be reminded again in 24 hours. If the application is still not installed after that, it will be installed automatically.
- **Schedule at** — Mac users will be required to install the application before the date and time specified here. If a user fails to install the application, it will be installed automatically.

11 Click **Next**.

12 On the **User Experience** page, select a notification type in the **User notification** drop-down list. Depending on the option selected, the following will happen when the application is ready to be installed on a Mac:

- **Display in Software Center and show all notifications** — The user will be asked to install the application and will have an option to start or postpone the installation. If the application is configured as **Available** (i.e. not required, see step 8 above) the user will have a choice not to install it. The application will be added to Application Portal where the user will be able to install it later. The installer graphical user interface will be displayed to the user providing full control over the installation process. When the installation is finished, the user will be asked to reboot the Mac if necessary.

- **Display in Software Center and only show notifications for computer restarts** — This option is similar to the **Display in Software Center and show all notifications** option (above) with one exception: the installer will run in the background, so the user will have no control over the installation process. The user will still be given a choice to install the application or to postpone the installation, and to restart or postpone restarting the Mac if it is required.
- **Hide in Software Center and all notifications** — The user will NOT be informed that the application is available for installation. The installation will be performed completely silently and transparently to the user. The application will NOT be added to Application Portal. If the installation requires Mac restart, the user will be asked to restart it and will be given an option to postpone restarting.

13 Complete the wizard using the default values and close it when done.

Installing Application on a Mac

When the application becomes available for installation on a Mac, the following will happen depending on the installation type deployment configuration options.

Installation is Optional

If the application is not required (the **Deploy Software Wizard** | **Deployment Settings** | **Purpose** is specified as **Available)**, a dialog will be displayed to the user describing the application and providing the following choices:

- **Show in Application Portal** — Clicking this button will open Application Portal where the user can view the application and install it if desired.
- **Install now** — Clicking this button will download the application and will run the application installer. The installer GUI will be displayed or hidden depending on the setting specified on the **User Experience** page of the **Deploy Software Wizard**.
- **Close** — Clicking this button will close the dialog. The user will be able to install the application later from Application Portal.

Installation is Required

If the application is required (the **Deploy Software Wizard** | **Deployment Settings** | **Purpose** is specified as **Required)** and an interactive installation type was specified, a dialog will be displayed to the user with the following options:

- **Postpone** — This button allows to postpone the installation. The **Remind me in** drop-down list allows to select the postponement period.

  Depending on the installation deadline setting (set in the **Deploy Software Wizard | Scheduling** page**)**, the following rules apply:

  - If the policy was downloaded prior to the installation deadline, the deadline will stay in effect.

  - If the policy was downloaded after the deadline has passed, the effective deadline will be set to the time of the policy download plus 24 hours.
- **Install now** — Clicking this button will close the dialog and will run the application installer.

Installation is Silent

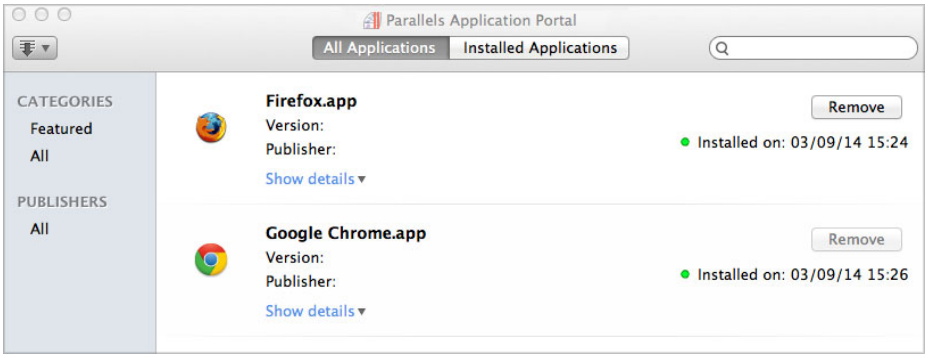
If the installation type was specified as silent (the **Deploy Software Wizard** | **User Experience page** | **Hide in Software Center and all notifications** option was selected), no message asking the user to install the application will be displayed, and the installation will be performed silently as soon as the policy is delivered to a Mac.

In all three scenarios above, after the application is installed, the user will be asked to reboot the Mac if the installer requires it or if the **Action** on the **User Experience** page of the **Mac OS X Properties** dialog is set to force a mandatory restart.

Using Parallels Application Portal

Parallels Application Portal is an OS X application included in the Parallels Mac Management for SCCM 2012 package. The application is installed on a Mac when Parallels Mac Client is installed on it.

To start Parallels Application Portal on a Mac, navigate to **Finder** > **Applications** and double-click **Parallels Application Portal**.



Parallels Application Portal allows the Mac user to:

- View and install applications made available to them by their system administrator.
- View and remove installed applications.
- Filter the applications by category and publisher.

For an application to be listed properly in Parallels Application Portal, it must be configured and deployed as described in **Application Management** and its subsections (p. 88).

When Application Portal starts, it should contain the list of the installed and available applications. If a Mac is not assigned to a Configuration Manager site, the application list will be empty.

The **Parallels Application Portal** window has the following elements:

- **All Applications** tab — Lists all application, including installed applications and applications that are available for installation. If at least one application was configured as "featured", the list will be split into two parts: **Featured Applications** and **Other Applications**. An application can be configured as "featured" on the **Application Catalog** tab page of the *<application_name>* **Properties** dialog (p. 90).

  If Configuration Manager has multiple versions of the same application that supersede each other, then only the top application will be displayed, unless the system administrator has specified the supersedence relationship on the **Supersedence** tab page of the *<application_name>* **Properties** dialog in the Configuration Manager console.
- **Installed Applications** tab — Lists applications that are installed on this Mac.
- **Categories** list — Contains software categories that the user can select to filter the application lists.
- **Publishers** list — Contains the names of software vendors that the user can select to filter the application lists.
- **Install** button — Displayed for applications that are available for installation. Clicking this button will download an application to the Mac and install it.
- **Remove** button — Displayed for an application already installed on a Mac. Allows to remove the application from the Mac. Please note that this button will only be available for applications that were configured in Configuration Manager as "Available" (i.e. optional, as opposed to required) and for which the uninstallation command line was specified. For more info about the installation/uninstallation command line, see **Configuring the Deployment Type** > **Specify the Installation Command Line** (p. 91).

Software Distribution

The software distribution feature automates the distribution of software to managed Mac computers. Software is distributed to Macs using the standard Configuration Manager functionality.

Creating Software Distribution Package

A software distribution package is a container for an application, file, or information that need to be applied to client Mac computers. A package also includes a program that contains instructions for how the contents of the package is to be applied on a client Mac. You create a package and a program using the standard **Create Package and Program Wizard** in the Configuration Manager console. Once the package is created, you can set additional package and program properties that are not available in the wizard. These properties can be used to better manage the installation process of the package on a Mac computer.

To create a package, in the Configuration Manager console, navigate to **Software Library / Overview / Application Management / Packages**. Click **Create Package**. The **Create Package and Program Wizard** opens. Populate the wizard pages as follows.

The Package page

14 Specify the package name and an optional description, manufacturer, language, and version information.

15 Select the **This package contains source files** option and then click the **Browse** button to select the source folder.

16 Click **Next**.

The Program Type page

Select the **Standard program** option and click **Next**.

The Standard Program page

1 Specify the program name.

2 Specify the command line for the program using the following rules:

- A command line that doesn't start with the colon (:) is treated as a standard Mac OS X shell command and is executed as-is. For example, to run the OS X installer(8) to install a .pkg package, the command line will look like this:

  ```
  installer -pkg "InstallMe.pkg" -target /
  ```

- To copy a directory from the distribution package to the Mac hard drive, use the following syntax:

  ```
  :<source_path>:<destination_path>:
  ```

  where <source_path> is the name and path of a directory inside the package, and <destination_path> is the name and path of a directory on a Mac. To reference directories inside an image file, the source path may contain the image file name (the file with the ".dmg" or ".iso" extension). For example, command line

  ```
  :firefox-8.0.1.dmg/Firefox.app:/Applications:
  ```

  will mount the firefox-8.0.1.dmg image to a temporary mount point and then copy the Firefox.app folder from that mount point to the /Applications folder on the Mac. The following example will do the same with the .iso image file

  ```
  :MySoft-image.iso/MyApp.app:/Applications:
  ```

- To run an installer command (Mac OS X package installer tool), use the following syntax:

  ```
  :<package_path>::
  ```

  where <package_path> is the name and path of the package. When the client encounters this command, it will invoke installer(8) passing the package name to it as a parameter. For example, command line

  ```
  :MySoft/MySoft-1.0.dmg/packages/mysoft_v1.pkg::
  ```

  will mount the MySoft-1.0.dmg image to a temporary mount point, make it current directory, and execute the following command:

```
$ /usr/sbin/installer -pkg "packages/mysoft_v1.pkg" -target /
```

The following example will similarly mount an .iso image file:

```
:MySoft/MySoft-1.0.iso/packages/mysoft_v1.pkg::
```

3 Specify whether you want to allow Mac users to interact with the program installation.

- To enable user interaction, in the **Run mode** drop-down list, select **Run with user's rights** or select the combination of the **Run with administrative rights** and **Allow users to view and interact with the program installation** options.
- To disable user interaction, set the **Run mode** option to **Run with administrative rights** and clear the **Allow users to view and interact with the program installation** option.

If you allow user interaction, a dialog will be displayed in OS X during program installation giving the user a choice to continue or to postpone installing the program. The message in the dialog will say whether an additional action, such as computer restart or user log-off, will be required (or may be required) after the program installation finishes. Based on this info, the user can decide whether to continue or to postpone the program installation. Please note that if a program installation is postponed, no other program can be installed before this one is installed first.

4 Click **Next**.

The Requirements page

Specify the following optional properties:

- **Estimated disk space**. Specifies the required disk space required to install the software on a target Mac. If a Mac doesn't have enough disk space, the software will not be installed on it and the Parallels Mac Client will report an error to the Configuration Manager.
- **Maximum allowed run time (minutes)**. Limits the maximum run time of the installation process. If the specified value is exceeded, the installation process is terminated and the failure is reported to the Configuration Manager.

Click **Next** and complete the wizard

Once the package is created, you can set additional package and program options that are not available in the wizard. The following subsections describe these options.

Specifying Actions to Perform After the Package Installation Finishes

You can configure the package program to restart a Mac or log off the user after the package installation finishes. Use these options when the software that you are distributing to Macs requires such actions to complete the installation.

To configure the program:

1 In the Configuration Manager console, select the package that you created and click the **Programs** tab at the bottom of the **Packages** workspace.

2 Select the program and click **Properties** on the toolbar. The program **Properties** dialog opens.

3 On the **General** tab, in the **After running** list, select the action that should be performed after the package installation finishes:

- **No action required.** This is the default option. If selected, no additional action will be performed on a Mac after the package installation finishes.
- **Configuration Manager restarts computer**. When this option is selected, a dialog box will be displayed in Mac OS X notifying the user that the Mac must be restarted. The user can postpone restarting if needed. If the action is postponed, the user will be reminded to restart the Mac later. If there are other packages waiting to be installed on the Mac, they will be installed only after the Mac is restarted.
- **Program controls restart**. Same as **No action required**.
- **Configuration Manager logs user off**. A dialog box will be displayed notifying the user that they have to log off to complete the installation. The user can postpone it if needed. If the action is postponed, the user will be reminded to log off later. The Parallels Mac Client will report success to the Configuration Manager even if the user postpones logging off the Mac as long as theinstallation completes without errors. The Mac Client will send the detailed installation results to the Configuration Manager as soon as the user logs off and then logs on again. If there are other packages waiting to be installed on the Mac, the installation will begin only after the user logs off and then logs on again.

See also **Create Package and Program Wizard** (p. 128)

Sending Package to Distribution Point

To distribute a package to client Macs, a copy of the package data must be sent to a distribution point from which the clients can download it.

To send a copy of the package to a distribution point, right-click the package of interest and click **Distribute Content** in the pop-up menu. Use the **Distribute Content Wizard** to specify a distribution point to which you want to send the package.

Please make sure that the distribution point is properly configured as described in the **Configuring a Distribution Point** section.

Deploying Software

After you've sent the package to a distribution point, you can deploy the software.

To deploy the software:

1 In the Configuration Manager console, right-click the package and then click **Deploy** in the pop-up menu. The **Deploy Software Wizard** opens.

2 On the **General** page, click the **Browse** button next to the **Collection** field and select the collection containing the desired Mac resources (e.g. **All Mac OS X Systems**). Click **OK** and then click **Next.**

3 On the **Content** page, verify the distribution point info and click **Next**.

4 Click **Next** on the **Deployment Settings** page.

5 On the **Scheduling** page, specify the schedule for this deployment. Click **New** to specify the assignment schedule. When done, click **Next**.

6 Use the default values on the rest of the wizard pages and complete the wizard.

The software will be advertised to Macs in the specified collection and will be distributed to them according to the schedule that you specified.

Viewing Status of a Package

While software distribution is in progress, the Mac Client running on target Mac computers will report to the Configuration Manager the following events:

- **Download started** — the event is reported when the client on a Mac begins downloading the software.
- **Download finished** — the event is reported when the package download is complete.
- **Download failed** — the event is reported if the package download fails.

To view the status of a package:

1 In the Configuration Manager console, navigate to **Monitoring / Overview / System Status / Deployments**.

2 In the right pane, right-click the package and then click **View Status** in the pop-up menu.

3 Use the **Deployment Status** view to examine the deployment status.

Deploying Mac OS X Images

The Mac OS X image deployment functionality allows to deploy Mac OS X on Mac computers. The following steps describes the Mac OS X image deployment procedure.

Step 1: Install Operating System Deployment (OSD) component

Parallels Mac Management includes a NetBoot Server component that must be installed and configured to enable the Mac OS X image deployment functionality. NetBoot is a technology from Apple that enables Mac computers to boot from a network. The NetBoot server is installed using the Parallels Mac Management installation wizard. If you skipped this option when you installed Parallels Mac Management, you can run the installation wizard and select the **NetBoot Server** option. For more information about installing and configuring the NetBoot server see **Prepare Your Computers for Installation** and **Install Parallels Mac Management for Microsoft SCCM** (p. 31).

Additionally, the Windows server running the Configuration Manager console must have the Windows Assessment and Deployment Kit (Windows ADK) installed. When installing ADK, make sure that the **Deployment Tools** option is selected.

Step 2: Create a bootable Mac OS X USB drive

You need a bootable Mac OS X USB drive to create a master and a slave partitions on a Mac to be imaged.

To create a bootable USB drive:

1. On a Mac running Mac OS X, mount the ".DMG" Mac OS X installation image file.
2. Navigate to `/Contents/SharedSupport/InstallESD.dmg`
3. Mount the `InstallESD.dmg` image.
4. Run **Finder > Applications > Utilities > Disk Utility**.
5. Select the hard disk and click **Restore** in the right pane.
6. Select `InstallESD.dmg/Mac OS X...` as **Source** and the USB drive as **Destination**.

You can also use a third-party utility to create a bootable USB drive, such as Lion DiskMaker.

Step 3: Prepare a reference Mac computer

Prepare a reference Mac computer to be imaged as follows:

1. On a Mac that doesn't have the operating system installed, boot from the USB drive (press the **Alt** key while restarting the Mac and choose the flash drive).
2. Run Disk Utility and install Mac OS X on the master partition.
3. After the the Mac OS X is installed, the Mac will reboot. When rebooting, press the **Alt** key and boot from the USB drive again.
4. Run Disk Utility and create a slave partition on the Mac. This step is necessary because you cannot create an image of the partition from which the operating system is running.
5. Install Mac OS X on the slave partition.
6. The Mac should now have two partitions: master and slave, each with Mac OS X installed.

Step 4: Create a Mac OS X disk image.

To create a Mac OS X disk image:

1. Boot from the slave partition (press the **Alt** key while restarting the Mac).
2. Run the System Image Utility (SIU), which is located in the `/Applications/Server` folder.
3. In the left pane, select the master partition as the source. In the right pane, select the **NetRestore Image** option. Click **Continue**.

4 In the **Network Disk** field, choose and type in the name for the image (e.g. `MyNetRestore`).

5 Click **Create** and choose a location on the slave partition. A folder containing the image will be created (e.g. `MyNetRestore.nbi`).

6 Copy the folder to the Windows server running the Configuration Manager console.

Step 5: Configure the OS X image in the Configuration Manager

In this step you need to convert the NBI image that you created earlier to the WIM format (Windows imaging) and add it to the Configuration Manager.

Use the **Add OS X Operating System Image Wizard** to convert the NBI image:

Note: To accomplish this task, you must run the Configuration Manager console with elevated user rights (**Run as Administrator**).

1 In the Configuration Manager console, navigate to **Software Library** / **Operating Systems** / **Operating System Images**.

2 Right-click **Operating System Images** and then click **Add Mac OS X Operating System Image** in the pop-up menu. The **Add OS X Operating System Image** wizard opens.

3 Specify the path to the OS X image (the folder with the ".nbi" extension) that you created earlier. The folder must be located in the local filesystem (if it's not, copy it to the local disk).

4 Specify the target path and filename for the ".wim" image. The path must be located on a network share. This is required because SCCM cannot create OS images from the local filesystem.

5 Click the **Next** button.

6 On the next page, specify the name for the image and an optional version and description. The image name must by unique on this Configuration Manager site.

7 Click **Next** and wait for the operation to finish.

8 Click **Finish** to close the wizard.

Note: If you are getting the **Error = 1314** message while trying to add the image, exit the Configuration Manager console and run it again using the **Run as Administrator** option.

Step 6: Create a collection of Mac computers to which the OS X image will be deployed

You can skip this step if you are deploying OS X to unmanaged Mac computers.

1 In the Configuration Manager console, navigate to **Assets and Compliance / Overview / Devices**. Right-click anywhere in the list and click **Import Computer Information** in the pop-up menu.

2 Provide a Mac computer name and MAC address and select **Add new computer only to the All Systems collection**.

3 On the new device record select **Add selected items to new device collection** to create new collection. Type the desired **Collection Name** and in **Limiting Collection** select **All Systems**.

Step 7: Create a Task Sequence associated with the OS X image

1 In the Configuration Manager console, navigate to **Software Library / Operating Systems / Task Sequences**.

2 Right-click anywhere in the list and click **Create Task Sequence for Macs** in the pop-up menu. The **Create Task Sequence for Macs** dialog opens.

3 Specify the name and an optional description for the new Task Sequence.

4 Click the **Browse** button and select the operating system image that you created earlier. Click **OK**.

5 Click **Finish** to exit the **Create Task Sequence for Macs** dialog.

You now need to distribute the OS X image referenced by the task sequence to a distribution point where the NetBoot server is installed.

To distribute the OS X image:

1 In the **Task Sequence** list, select the task sequence that you just created.

2 On the **Home** tab, in the **Deployment** group, click **Distribute Content** to start the Distribute Content Wizard.

3 On the **General** page, verify that the correct task sequence is selected for distribution, and then click **Next**.

4 On the **Content** page, verify the content to distribute (the OS X image referenced by the task sequence) and then click **Next**.

5 On the **Content Destination** page, specify the distribution point where the NetBoot server is installed. Click **Next** and complete the wizard.

You can now deploy the task sequence as follows:

1 In the **Task Sequence** list, right-click the task sequence and click **Deploy** in the pop-up menu.

2 Select the collection that contains Mac computers that will run the task sequence. If you are deploying OS X to unmanaged Macs, select the **All Mac OS X Systems** collection.

Note: The NetBoot server can deploy an OS X image on Macs assigned to the SCCM site (managed Macs) and to Macs that are not assigned (unknown Macs). The unknown Mac support is turned on or off using the **Support for unknown Macs** page of the **Parallels NetBoot Server Configuration Wizard**. You can run the wizard at any time to turn this feature on or off. If the unknown Mac support is turned off, the NetBoot server will ignore the unassigned Macs and will deploy the image on managed Macs only. If the feature is turned on, the image will be deployed on both assigned and unassigned Macs.

Step 8: Start up a Mac from the NetBoot server

To start up a Mac using the disk image:

- If you have a single OS X image, you can hold the **N** key as a Mac boots to boot from it.
- If you have multiple images, hold the **Option** key during the Mac startup. This will start the Mac in **Startup Manager** where you can select an image to boot from.

Deploying Parallels Desktop and Virtual Machines on Macs

Parallels Desktop for Mac is a virtualization software that allows to run Windows and other operating systems on a Mac computer alongside Mac OS X. With Parallels Mac Management you can remotely deploy Parallels Desktop to managed Mac OS X computers. Deploying Parallels Desktop to Macs is similar to distributing other software: you create a distribution package, add a program to it, copy the package to a distribution point, and create an advertisement (see **Software Distribution** (p. 97)). The Parallels Desktop deployment adds a few extra steps, which are described below.

Preparing a Deployment Package

Parallels provides a special software package that can be used to mass deploy Parallels Desktop to many Macs at once. Normally, this package is used for deploying Parallels Desktop in a Mac-only environment. It can also be used to distribute Parallels Desktop using Parallels Mac Management.

To prepare the deployment package:

1. Download the package from http://download.parallels.com/desktop/tools/pd-autodeploy.zip to your Windows server where the Configuration Manager console is running.
2. Unzip the file. You should now see the `Parallels Desktop Autodeploy.pkg` folder.
3. Navigate to `Parallels Desktop Autodeploy.pkg\Parallels` folder, which should contain a single file named `License.txt`.
4. Open the file in a text editor, type your Parallels Desktop license number, and save it. You can type the license number on any line in the file. The number must be specified using the following format: XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX. Please note that the license must allow to install Parallels Desktop on the planned number of Macs.
5. Copy the Parallels Desktop installation disk image (.dmg file) to the `Parallels Desktop Autodeploy.pkg\Parallels` folder where the `License.txt` file is residing.

Adding Virtual Machines to the Deployment Package

If you would like to distribute one or more virtual machines together with Parallels Desktop, you have to add them to the deployment package. To include a virtual machine, locate the virtual machine bundle (the file with the .pvm extension) and simply copy it to the `Parallels Desktop Autodeploy.pkg\Parallels` folder (the same folder where the Parallels Desktop image and the `License.txt` files are residing).

Parallels Desktop and a source virtual machine can be configured before deployment in a number of ways according to your requirements. This includes the general virtual machine configuration parameters, such as the number of CPUs, available RAM, hard disk size, etc., as well as additional configuration options. For instance, you may want to modify the default virtual machine location, install Parallels Tools in a virtual machine, set up automatic Windows SID generation, and do other customization. For more information on how to customize Parallels Desktop and a source virtual machine, please read the **Parallels Desktop Mass Deployment and Management** guide, which can be downloaded from the Parallels Web site.

Note: The `Parallels Desktop Autodeploy.pkg` package will not automatically register Parallels Desktops deployed to remote Macs. If your license allows to run Parallels Desktop simultaneously on several Macs, all you have to do is register it once on one Mac. If you have individual licenses, you'll have to manually activate Parallels Desktop and register it on every Mac to which it was deployed. Parallels Desktop can also be purchased through the Parallels Volume Licensing program. If you have such a license, you don't have to register Parallels Desktop and still get all the benefits of a registered product.

Creating a Software Distribution Package

The Parallels Desktop deployment package is distributed to Macs using the standard Configuration Manager functionality:

1. In the Configuration Manager console, navigate to **Administration / Overview / Application Management / Packages**.
2. On the toolbar, click **Create Package**.
3. Use the **Create Package and Program Wizard** to create a software distribution package and a program.
4. On the **Package** page, specify the package name, description, and other information. Select the **This package contains source files** option and then click the **Browse** button. Browse for and select the `Parallels Desktop Autodeploy.pkg` folder. When done, click **Next**.
5. On the **Program Type** page, select the **Standard program** item and click **Next**.
6. On the **Standard Program** page, specify the information about the program. Type the following in the **Command line** field:

   ```
   chmod 700 "Parallels Desktop
   Autodeploy.pkg/Contents/Resources/postflight" && installer -pkg
   "Parallels Desktop Autodeploy.pkg" -target /
   ```

7. When done specifying the program information, click **Next**.
8. Click **Next** on the **Requirements** page.
9. Review the summary and click **Next** to create the package.

Sending the Package to a Distribution Point

To send a copy of the package to a distribution point, right-click the package of interest and click **Distribute Content** in the pop-up menu. Use the **Distribute Content Wizard** to specify a distribution point to which you want to send the package.

Please make sure that the distribution point is properly configured as described in the **Configuring a Distribution Point** section.

Deploying Parallels Desktop

To deploy Parallels Desktop:

1. In the Configuration Manager console, right-click the package and then click **Deploy** in the pop-up menu. The **Deploy Software Wizard** opens.
2. On the **General** page, click the **Browse** button next to the **Collection** field and select the collection containing the desired Mac resources (e.g. **All Mac OS X Systems**). Click **OK** and then click **Next.**
3. On the **Content** page, verify the distribution point info and click **Next**.
4. Click **Next** on the **Deployment Settings** page.
5. On the **Scheduling** page, specify the schedule for this deployment. Click **New** to specify the assignment schedule. When done, click **Next**.
6. Use the default values on the rest of the wizard pages and complete the wizard.

The package will be advertised to Macs in the specified collection and will be distributed to them according to the schedule that you specified.

See also **Viewing the Status of a Package** (p. 101) for the information on how to see the package distribution results.

Deploying SCCM Client in Windows Running in a Virtual Machine

If your Mac computers are hosting Windows running in a Parallels virtual machine, you can install Configuration Manager 2012 client software in Windows and manage it the same way as Windows running on physical computers. Parallels Mac Management provides functionality that helps you automates the deployment of Configuration Manager 2012 client software to Windows running in a virtual machine.

The Configuration Manager 2012 client software is deployed to Windows using the Parallels Mac Management software distribution feature. The steps involved in the procedure are similar to Mac software distribution:

1. Configure a distribution point.
2. Create a software distribution package (see below).
3. Create a program (see below).
4. Send the package to the distribution point.
5. Deploy the software.

The rest of this section describes how to create a software distribution package and a program containing instructions to install the client software in Windows. Please follow the links in the list above for the information on how to perform the other steps.

Before creating a package, verify that the following requirements are met:

- Windows running in a Parallels virtual machine is a member of the same domain as the Configuration Management 2012 site.
- Windows has Parallels Tools installed.

Creating a Software Distribution Package

A software distribution package is a container for an application, file, or information that need to be applied to client computers. In this instance, the package will contain Configuration Manager 2012 client software and a special file containing command-line instructions that you have to create prior to creating a package.

To create a command line file, on the computer running the Configuration Manager console, navigate to the `C:\Program Files (x86)\Microsoft Configuration Manager\Client` directory. The directory should contain Configuration Manager 2012 client software. Create a text file in the directory and name it `install_agent_for_vm.cmd`. Copy and paste the following instructions into the file:

```
ccmsetup /noservice SMSSITECODE=<sitecode> CCMDEBUGLOGGING=1
CCMENABLELOGGING=TRUE CCMLOGLEVEL=0 SMSDIRECTORYLOOKUP=NOWINS SMSMP=<mp
hostname>
```

The command line above uses two variables: `<sitecode>` and `<mp hostname>`. Substitute the variables as follows:

- `<sitecode>` — substitute with the Configuration Manager site code.
- `<mp hostname>` — substitute with the Management Point hostname.

Create a distribution package and a program as described in the **Software Distribution** section. When creating a package, specify the Configuration Manager 2012 client Agent directory as the source. When specifying the command line for a program, use the following line:

```
:::osname=^Windows.*$!vmname=^.*$!checkversion=%SYSTEMROOT%\CCM\LSInter
face.dll|4.0.6487.2177!cmdline= install_agent_for_vm.cmd
```

When the package is created, send it to a distribution point and specify the deployment settings. See **Software Distribution** (p. 97) for details.

Managing Windows Virtual Machine

After you install the Configuration Manager client agent in a Windows virtual machine, the machine can be managed from the Configuration Manager console. Please note that depending on the networking mode used by the virtual machine, some of the standard SCCM management functions may not work. Please read the explanation below.

A Parallels virtual machine can be configured to operate in one of the following networking modes:

- **Host-only**. This networking mode completely hides the virtual machine from the outside world, so it cannot be managed by the Configuration Manager.
- **Bridged**. This mode makes the virtual machine appear on your local network and the Internet as a standalone computer, so it can be fully managed by the Configuration Manager just like a physical Windows machine.
- **Shared**. A machine that operates in this mode has full network access, but cannot be accessed by other computers on your network. This means that the Configuration Manager features that need to connect to the virtual machine will not work. For example, the Remote Tools feature will not work. However, the SCCM client agent running in a virtual machine can communicate with the Configuration Manager, so features like software distribution, desired configuration management, hardware and software inventory will work. In general, if a management task is initiated and performed by the client agent, it will work. If a task is initiated on the Configuration Manager site and then tries to connect to the client agent running in a virtual machine, it will not work.

To set the networking mode for a Parallels virtual machine, open the virtual machine in Parallels Desktop, select **Virtual Machine** in the Parallels Desktop menu, and click **Configure**. In the virtual machine configuration dialog, click the **Hardware** tab and then select **Network 1** (or the network adapter of interest) in the list. Use the **Type** drop-down list box to set the network type.

Providing Remote Assistance to Mac Users

The Remote Assistance feature allows a system administrator to temporarily connect to a remote Mac computer and correct any problems on it if necessary. A remote connection can be established right from the Configuration Manager console with both managed and unmanaged Macs.

To use the Remote Assistance feature, open the Configuration Manager console, find a Mac that you want to connect to and right-click it. In the pop-up menu, point to **Parallels Management Tools**, and click one of the following connection options:

- **Connect via VNC**. This option uses the Virtual Network Computing graphical desktop sharing system, which lets you remotely control the Mac OS X desktop.

- **Connect via SSH**. This option uses the Secure Shell (SSH) protocol to access a shell account on a remote Mac and execute commands in Mac OS X.

Parallels Mac Management uses third-party VNC and SSH client utilities that are installed in Windows automatically when you install the Configuration Manager Console Extension component. A VNC server and an SSH server are included in every edition of Mac OS X and are installed on a Mac by default. The following describes how to set up and use each connection option.

Connect via VNC

Before using this feature, the Mac OS X Remote Management service must be enabled on each individual Mac.

To enable Mac OS X Remote Management:

1. Log in to a Mac.
2. Open System Preferences.
3. Choose **View > Sharing**, or click Sharing.
4. In the Service list, select Remote Management and enable it by selecting the On checkbox.
5. Click the **Computer Settings** button and then select the **VNC viewers may control screen with password** checkbox.
6. Choose a VNC password and enter it in the field provided. You will later use the password to establish a VNC connection with the Mac. Whether you choose the same VNC password for all Macs in your enterprise (for simplicity) or a unique password on each Mac depends on your security policies.
7. Click **OK**.
8. Close System Preferences.

When you select the **Connect via VNC** option in the Configuration Manager console, the VNC viewer application starts and asks you to enter the Mac user ID and the VNC password. If the credentials are valid, a window is displayed where you can remotely control the Mac OS X desktop.

Connect via SSH

Before using this feature, the SSH service must be enabled on each individual Mac.

To enable SSH in Mac OS X:

1. Log in to a Mac.
2. Open System Preferences.
3. Choose **View > Sharing**, or click Sharing.
4. In the Service list, select Remote Login and enable it by selecting the On checkbox.
5. Close System Preferences.

When you select the **Connect via SSH** option in the Configuration Manager console, the SSH client application starts and asks you to enter the Mac user ID and password. If the credentials are valid, an SSH window opens where you can type and execute commands in Mac OS X.

Problem Reporting and Monitoring

The Parallels Mac Management reporting functionality helps you to gather system information for the Configuration Manager Proxy, Configuration Manager Console Extension, and managed Mac computers. The collected information can then be sent to Parallels Support. The following subsections describe how to use the Parallels Mac Management problem reporting tools and utilities.

Sending Problem Reports Using Configuration Manager Console

Configuration Manager Console Extension provides a reporting feature that can be used to collect information about managed Mac OS X computers. If you have a problem with a Mac, you can generate a report and send it to Parallels Support for analysis.

To access the reporting feature, open the Configuration Manager console, navigate to the Mac you're having a problem with, right-click it and select **Parallels Management Tools > Send Problem Report**. In the **Problem Report for Parallels Mac Management for Microsoft SCCM** dialog, type a message that will be appended to the report and then click **Send Report**. A window with a progress bar will open informing you of the information gathering progress. The process consists of the following steps (transparent to the user):

1. The Configuration Manager Console Extension information is collected and is sent to the Configuration Manager Proxy together with the selected Mac identifier.
2. The Configuration Manager Proxy collects its own data and then requests the data from the specified Mac computer.
3. The client software on the Mac collects its data and sends it back to the Configuration Manager Proxy.
4. The Configuration Manager Proxy merges individual reports into a single one and sends it to Parallels Support.

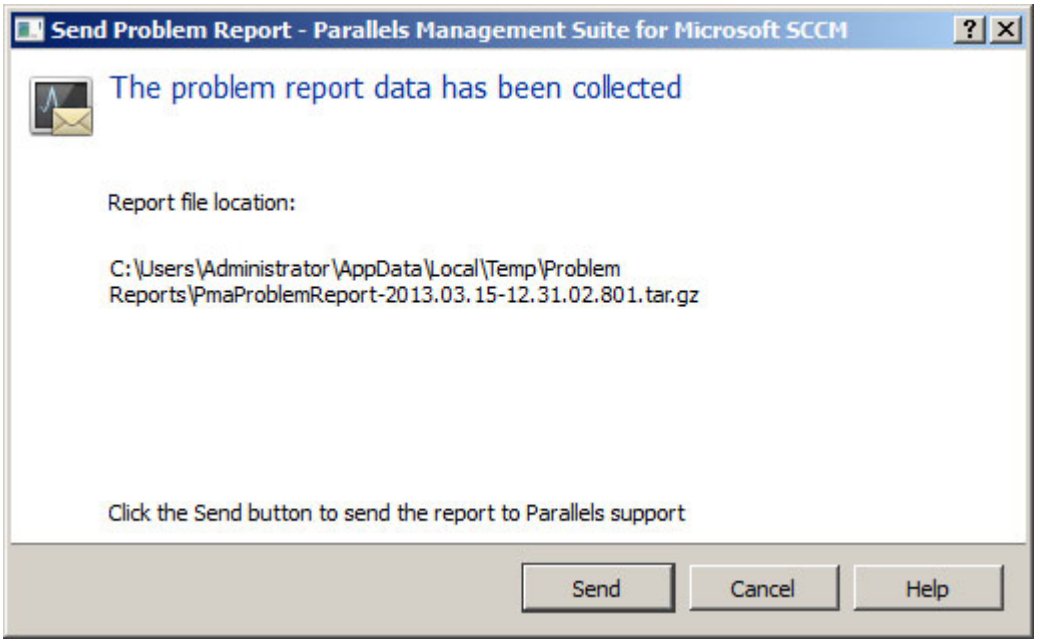
The final report will contain combined information gathered from all three components: Configuration Manager Proxy, Console Extension, and the Mac that was selected. After the problem report is sent to Parallels, a dialog will open displaying the report ID. If you would like to request help with the issue, you can submit a ticket to Parallels Support and include this ID for reference.

If you receive an error while using the reporting feature, make sure that the Configuration Manager Proxy and the Mac are running and accessible. If for some reason you cannot start or access the Configuration Manager Proxy or the Mac, you can use the available standalone reporting utilities, which are described in the following section.

Sending Problem Reports Using Windows Reporting Utility

In addition to the Configuration Manager Console Extension reporting feature, Parallels Mac Management provides a standalone reporting utility for Windows, which is installed when you install the Configuration Manager Proxy or the Configuration Manager Console Extension components. Compared to the Configuration Manager console reporting feature, this utility will collect information for individual Parallels Mac Management components. For example, if you run the utility on the computer where the Configuration Manager Proxy is installed, the information will be gathered for the Configuration Manager Proxy only. If you run it on the computer where the Configuration Manager Console Extension is installed, the information will be gathered for the Console Extension. If both components are installed on the same computer, both will be included in the report.

To run the utility, go to **Start > All Programs > Parallels > Parallels Mac Management for Microsoft SCCM** and click the **Send Problem Report** item. The **Send Problem Report** dialog opens and the data gathering process begins. Once the report is generated, a message is displayed in the dialog specifying a temporary location on the local hard drive where the report file was saved.


Send Problem Report - Parallels Management Suite for Microsoft SCCM
The problem report data has been collected
Report file location:
C:\Users\Administrator\AppData\Local\Temp\Problem Reports\PmaProblemReport-2013.03.15-12.31.02.801.tar.gz
Click the Send button to send the report to Parallels support
Send
Cancel
Help

Click the **Send** button to send the report to Parallels Support. After the report is sent, a message box containing the problem report number is displayed. You can use this number for future reference. The report file is automatically deleted from the temporary location.

Click **Cancel** to close the dialog without sending the report. If the utility is run on the computer where the Configuration Manager Proxy is installed, the report file will be forwarded to Configuration Manager Proxy, which will notify the Problem Monitor about it. You can then use the Problem Monitor to view the report summary and to send it to Parallels Support. For the information about Problem Monitor, see **Using Problem Monitoring Utility** (p. 113). If the utility is run on the computer where only the Configuration Manager Console Extension is installed, the report file will be deleted from the temporary directly and no other actions will be performed.

Sending Problem Reports from Mac Client

A reporting utility is installed on a Mac computer during the Parallels Mac Client software installation. To run the utility, open **System Preferences** and then click **Parallels Management** (if your **System Preferences** are organized by categories, it is located in the **Other** category). For more information about using the utility, see **Sending Mac Client Problem Report** (p. 55).

Using Problem Monitoring Utility

Parallels Mac Management for Microsoft SCCM 2012 provides a utility that allows to monitor the system in real time for possible problems. The utility is installed together with Parallels Mac Management and can be accessed on computers where the Configuration Manager Proxy or the Configuration Manager Console Extension are installed.

The problem monitor runs in the background with a notifier in the Windows taskbar notification area (also called the "system tray"). It receives problem report notifications from the Configuration Manager Proxy and notifies the IT administrator when the reports are available. The following list describes how the monitor interacts with the Configuration Manager Proxy and the administrator:

1. If there's a problem with Parallels Mac Management, the Configuration Manager Proxy generates a report, saves it to a local file, and sends a notification to the problem monitor that a new report is available.
2. The problem monitor receives the notification and displays a balloon tip in the notification area informing the administrator of a new report.
3. The administrator can open the problem report list, which is populated with the names of the available reports and some basic info about them.
4. The administrator can then send a report to Parallels Support, delete it, or close the list and return to it later.

The rest of this section describes how to use the problem monitor.

Starting and Stopping the Problem Monitor

The monitor starts automatically after you complete the Parallels Mac Management installation. It also starts automatically when the computer is rebooted and a user logs in to Windows. If the user is not authorized to access the computer where the Configuration Manager Proxy is running, a dialog is displayed asking the user to enter a user name and password. After the problem monitor is connected to the Configuration Manager Proxy, it adds a notifier to the taskbar notification area.

To terminate the problem monitor, right click its icon in the notification area and select **Quit** from the pop-up menu. To manually start the monitor, go to **Start** > **All Programs** > **Parallels** > **Parallels Mac Management for Microsoft SCCM** and click **Problem Monitor**. When the monitor starts, it immediately requests problem report information from the Configuration Manager Proxy. If there are new problem reports, a balloon tip is displayed.

Receiving Problem Monitor Notifications

By default the problem report icon in the notification area is hidden. To make it always appear, right-click the notification area and select **Customize notification icons** in the pop-up menu. Change the behavior of the Problem monitor utility to "Show icons and notifications".

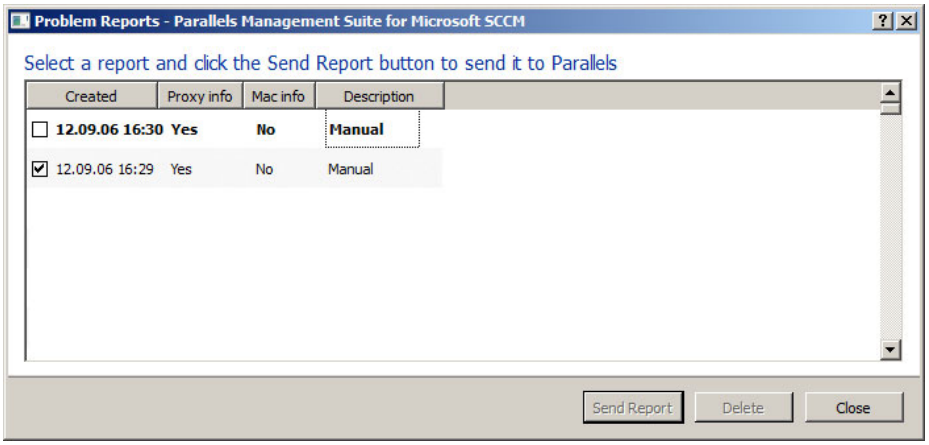
Depending on the problem monitor status, its icon will be one of the following:

- indicates that there are no new problem reports.
- indicates that one or more new problem reports are available.
- indicates that the problem monitor cannot communicate with the Configuration Manager Proxy. This can happen if the Configuration Manager Proxy is down or if there's a network problem.

The problem monitor communicates with the Configuration Manager Proxy every one minute. If there's a new problem report, the proxy notifies the monitor. Once the notification is received, the problem monitor displays a balloon tip in the notification area and its icon changes accordingly.

Viewing the Problem Report List

To view the problem report list, click the balloon to open the **Problem Reports** dialog. If the balloon is not currently displayed, right-click the problem monitor icon and select **Show Problem Reports** from the pop-up menu (or you can simply click the icon).



Each row in the list contains information about an individual report and has the following columns:

- **Created** — contains the date and time when the report was created.
- **Proxy info** — if set to "Yes", indicates that the report contains the information related to the Configuration Manager Proxy.
- **Mac info** — if set to "Yes", indicates the the report contains the information related to a managed Mac computer.
- **Description** — specifies whether the report was generated automatically or manually by a user.

If there are no problem reports on the server, the list will be empty.

To perform an action on a report, select the report of interest from the list and click one of the available buttons:

- Click **Send** to send the selected problem report to Parallels Support. After the report is sent, it is removed from the server on which it resides.
- Click **Delete** to delete the selected report from the list and the server on which it resides.
- Click **Close** to closes the dialog. The reports will remain in the problem monitor report list and the report files will remain in their original locations.

Viewing the Problem Report Activity Log

The problem monitor maintains an activity log, which contains the information about the operations that were performed on the reports. To view the problem report activity log, right-click the problem monitor icon in the notification area and select **Problem Reports Log** from the pop-up menu. The **Problem Report Operations Log** dialog opens. Each entry in the log describes an individual operation that was performed on a report. This is a read-only information provided as a reference. If a report operation included sending it to Parallels Support, the entry will include the report ID, which can be used when following up on the report with Parallels Support.

Tracking Apple Warranty Status of Macs

Parallels Mac Management allows you to track the Apple warranty status of each enrolled Mac. The warranty information is collected when a Mac is assigned to the Configuration Manager site and is saved in the Configuration Manager database. The database record is then updated according to the hardware inventory schedule.

Note: To collect the Apple warranty information, make sure that Hardware Inventory is configured properly. See **Configuring Inventory Settings** (p. 58) for details.

To view the Apple warranty information for a specific Mac:

1. In the Configuration Manager console, navigate to the collection containing your Mac computers.
2. Right-click the Mac of interest and select **Start** > **Resource Explorer** in the context menu.
3. In the **Resource Explorer** window, expand the **Hardware** node and click **Apple Warranty Info**.
4. The following Apple warranty info is displayed in the right pane:
   - **Serial Number** — the Mac's serial number.
   - **Warranty Expires** — the warranty expiration date. If a Mac is out of warranty, this column will not be shown.
   - **Warranty Status** — the Apple warranty status. If the Mac is out of warranty, the status will be "Out of Coverage".

Parallels Mac Management also creates a report containing the Apple warranty information for all managed Mac computers. The report can be viewed in the Configuration Manager console at the following location: **Monitoring** / **Reporting** / **Reports** / **Hardware General** / **Apple Warranty Info**.

The **Apple Warranty Info** report contains the following information:

- **Name** — resource name (same as the device name in the device collection).
- **Resource** — SCCM resource ID.
- **Serial Number** — Mac's serial number.

- **Status** — Apple warranty status.
- **Expiration Date** — Apple warranty expiration date.
- **Last Update** — the date on which the warranty information was last updated.

CHAPTER 6

Technical Reference

This chapter provides the resources to help you use the Parallels Mac Management user interface components.

In This Chapter

Wizard Pages 118
Property Pages 129
Dialog Pages 134

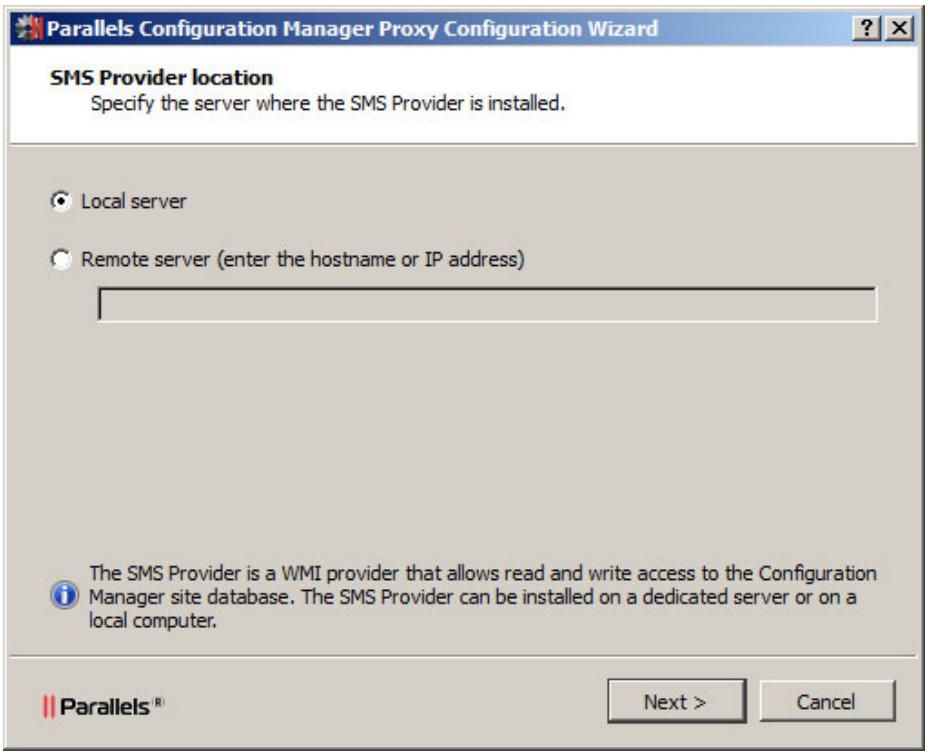
Wizard Pages

Parallels Configuration Manager Proxy Configuration Wizard

The **Configuration Manager Proxy - Configuration utility** wizard is used to configure the Configuration Manager Proxy service.

SMS Provider Location Page

The **SMS Provider location** page is used to specify the IP address or hostname of the server where the SMS Provider is installed.


Parallels Configuration Manager Proxy Configuration Wizard
SMS Provider location
Specify the server where the SMS Provider is installed.
Local server
Remote server (enter the hostname or IP address)
The SMS Provider is a WMI provider that allows read and write access to the Configuration Manager site database. The SMS Provider can be installed on a dedicated server or on a local computer.
Parallels
Next >
Cancel

The page contains the following elements:

Local Server

Select this option if the SMS Provider is installed on the server where you are running this wizard.

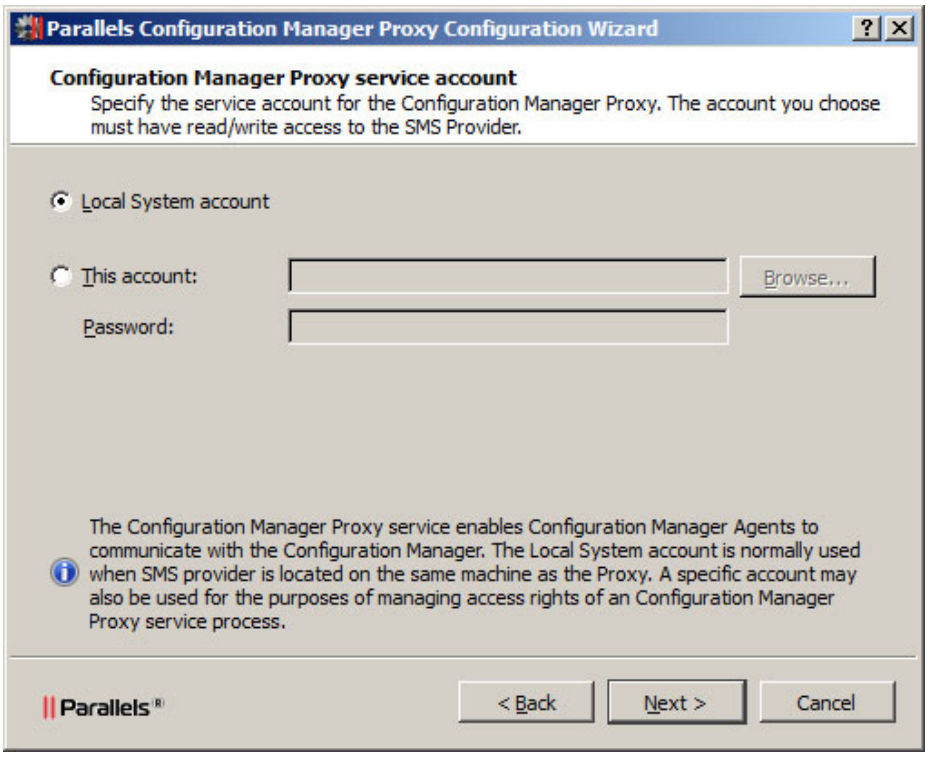
Remote server (enter the server hostname or IP address)

Select this option if the SMS Provider is running on a remote server. Enter the server IP address or hostname in the text field provided.

Configuration Manager Proxy Service Account Page

The **Configuration Manager Proxy service account** page is used to specify a user account, which will be used to run the Configuration Manager Proxy service.

Note: The Configuration Manager Proxy service account must have read/write access to the SMS Provider.


Parallels Configuration Manager Proxy Configuration Wizard
Configuration Manager Proxy service account
Specify the service account for the Configuration Manager Proxy. The account you choose must have read/write access to the SMS Provider.
Local System account
This account:
Browse...
Password:
The Configuration Manager Proxy service enables Configuration Manager Agents to communicate with the Configuration Manager. The Local System account is normally used when SMS provider is located on the same machine as the Proxy. A specific account may also be used for the purposes of managing access rights of an Configuration Manager Proxy service process.
Parallels
< Back
Next >
Cancel

The page contains the following elements:

Local System account

Specifies that the predefined LocalSystem account should be used to run the Configuration Manager Proxy service.

This account

Specifies a user account name. This can be a local or a domain user account. Enter the account name into the text field provided.

- **Browse** button — opens the standard Windows user account selection dialog where you can select an account from the list.
- **Password** — specifies the account password.

Management Point Location and SCCM Site Code Page

The **Management Point location and SCCM site code** page is used to specify the Management Point hostname and the Configuration Manager site code.

Note: The page is only displayed when there is more than one Management Point in your system. If you have a single Management Point, its address will be determined automatically and the page will not be displayed.

The page has the following elements:

SCCM site code

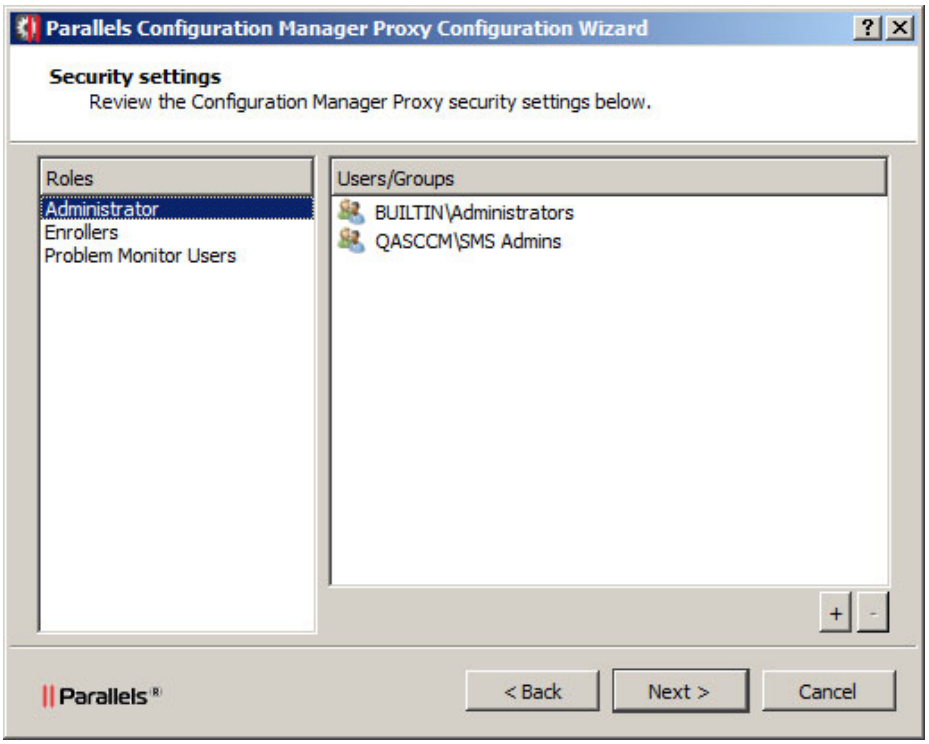
Specifies the Configuration Manager site code. Select the site code that you want to use from the list.

Security Settings Page

The **Security settings** page is used to configure the Configuration Manager Proxy role-based access control. The roles are created during the Parallels Mac Management installation and include the following:

- **Administrator**. This role provides access to all of the available Configuration Manager Proxy functions, including Mac registration, Mac management via the Configuration Manager console, problem monitoring functions, and others.
- **Enrollers**. This role provides access to the Mac registration functionality. A Mac computer must be registered with the Configuration Manager Proxy before it can be managed via the Configuration Manager console. Members of this role are allowed to run the Mac registration utility on a Mac and register it with the Configuration Manager Proxy.
- **Problem Monitor Users**. This role provides access to the Parallels Mac Management problem monitoring functions. Problem Monitor is a service that monitors the system in real time for possible problems. Members of this role are allowed to use problem monitoring functions, including running the Problem Monitor, viewing reports, deleting reports, and others.

The roles are listed in the **Roles** list. You can select a role and see the default users and groups for it. Depending on your requirements, you can remove a default group and/or add a new group or a user. To remove a group, select it and click the "-" button. To add a group or a user click the "+" button and use the standard **Select Users, Computers, Service Accounts, or Groups** dialog to specify a user or a group.



The page contains the following elements:

Roles

Lists the existing security roles.

Users/Groups

Lists users and groups for the selected role.

+ button

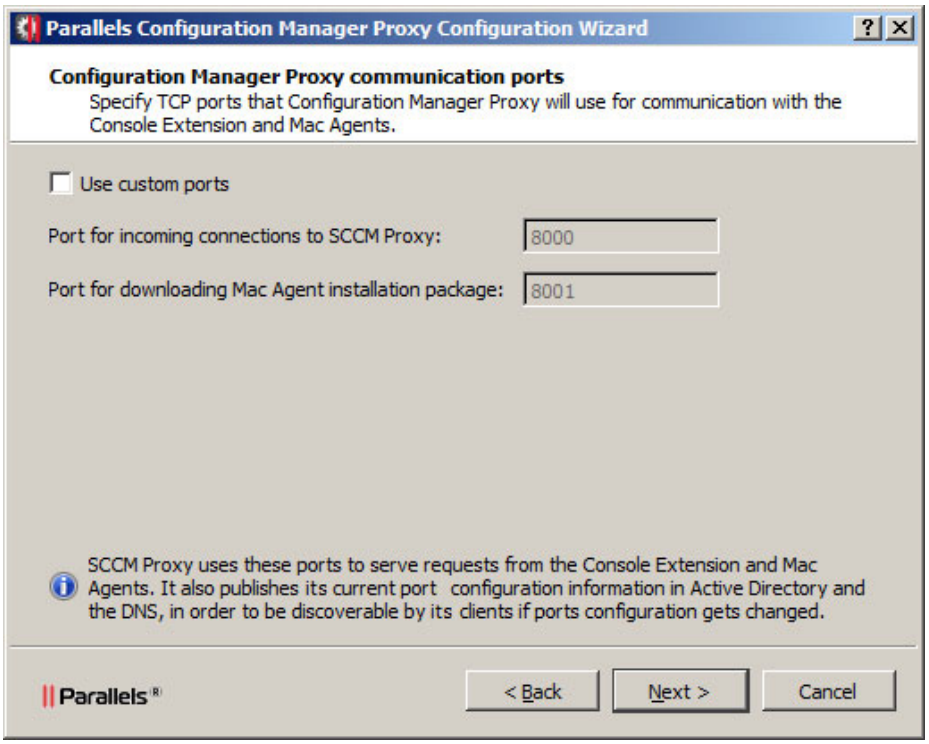
Click this button to add a user or a group to the selected role.

- button

Click this button to remove a user or a group from the selected role.

Configuration Manager Proxy Communication Ports Page

The **Configuration Manager Proxy communication ports** page can be used to change the default communication ports.


Parallels Configuration Manager Proxy Configuration Wizard
Configuration Manager Proxy communication ports
Specify TCP ports that Configuration Manager Proxy will use for communication with the Console Extension and Mac Agents.
Use custom ports
Port for incoming connections to SCCM Proxy:
8000
Port for downloading Mac Agent installation package:
8001
SCCM Proxy uses these ports to serve requests from the Console Extension and Mac Agents. It also publishes its current port configuration information in Active Directory and the DNS, in order to be discoverable by its clients if ports configuration gets changed.
Parallels
< Back
Next >
Cancel

The page contains the following elements:

Use custom ports

Select this option to override the default communication ports.

Ports for incoming connections to SCCM Proxy

Displays the default port used by SCCM Proxy for incoming connections. When the **Use custom ports** option is selected, this field is used to specify a custom port.

Port for downloading Mac Agent installation package

Displays the default port used to download Parallels Mac Client installation image. When the **Use custom ports** option is selected, this field is used to specify a custom port.

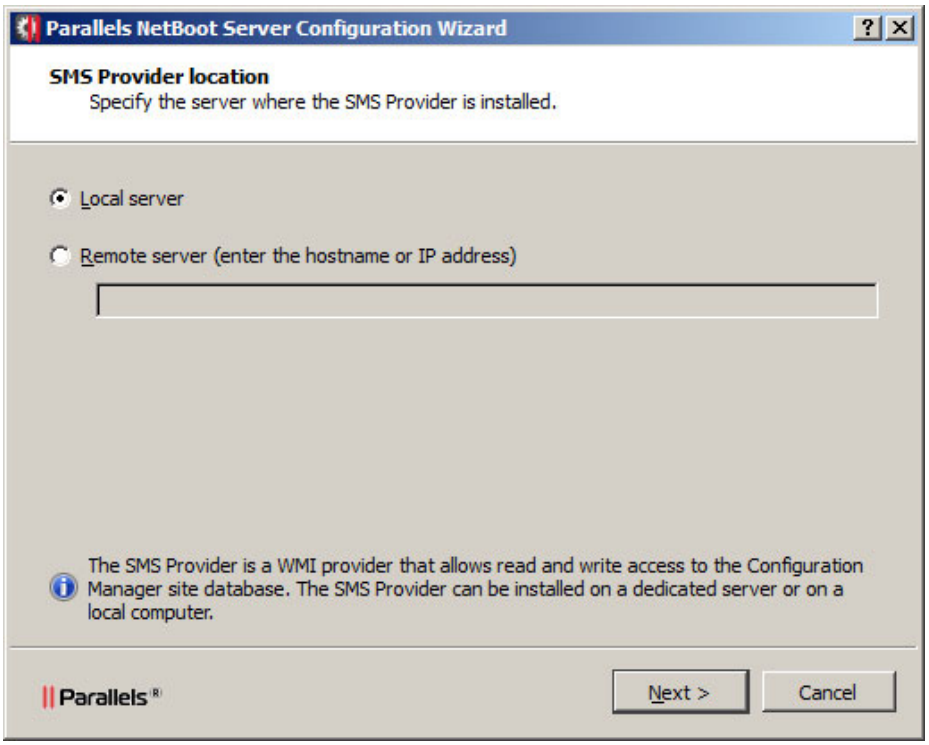
Configuration Settings Summary Page

The **Configuration settings summary** page displays the Configuration Manager Proxy configuration summary. Review the settings and click **Finish** to apply them or click **Back** to return to the previous page.

Parallels NetBoot Server Configuration Wizard

SMS Provider Location Page

The **SMS Provider location** page is used to specify the IP address or hostname of the server where the SMS Provider is installed.


Parallels NetBoot Server Configuration Wizard
SMS Provider location
Specify the server where the SMS Provider is installed.
Local server
Remote server (enter the hostname or IP address)
The SMS Provider is a WMI provider that allows read and write access to the Configuration Manager site database. The SMS Provider can be installed on a dedicated server or on a local computer.
Parallels
Next >
Cancel

The page contains the following elements:

Local Server

Select this option if the SMS Provider is installed on the server where you are running this wizard.

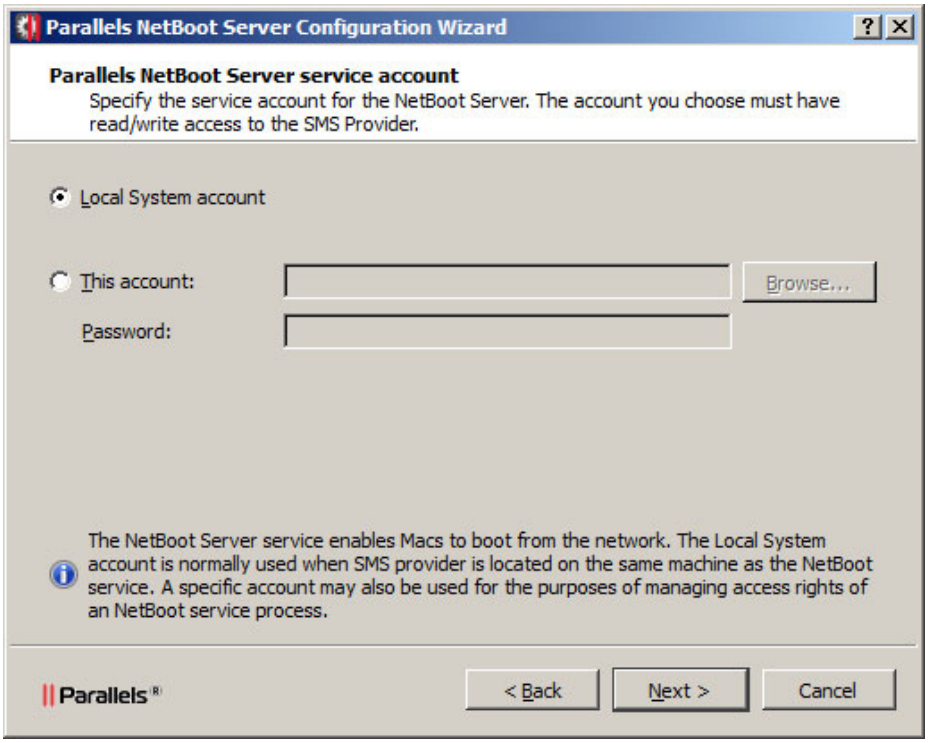
Remote server (enter the server hostname or IP address)

Select this option if the SMS Provider is running on a remote server. Enter the server IP address or hostname in the text field provided.

Parallels NetBoot Server Service Account page

The **Parallels NetBoot Server service account** page is used to specify a user account, which will be used to run the NetBoot service.

Note: The account must have read/write access to the SMS Provider.


Parallels NetBoot Server Configuration Wizard
Parallels NetBoot Server service account
Specify the service account for the NetBoot Server. The account you choose must have read/write access to the SMS Provider.
Local System account
This account:
Browse...
Password:
The NetBoot Server service enables Macs to boot from the network. The Local System account is normally used when SMS provider is located on the same machine as the NetBoot service. A specific account may also be used for the purposes of managing access rights of an NetBoot service process.
Parallels
< Back
Next >
Cancel

The page contains the following elements:

Local System account

Specifies that the predefined LocalSystem account should be used to run the Configuration Manager Proxy service.

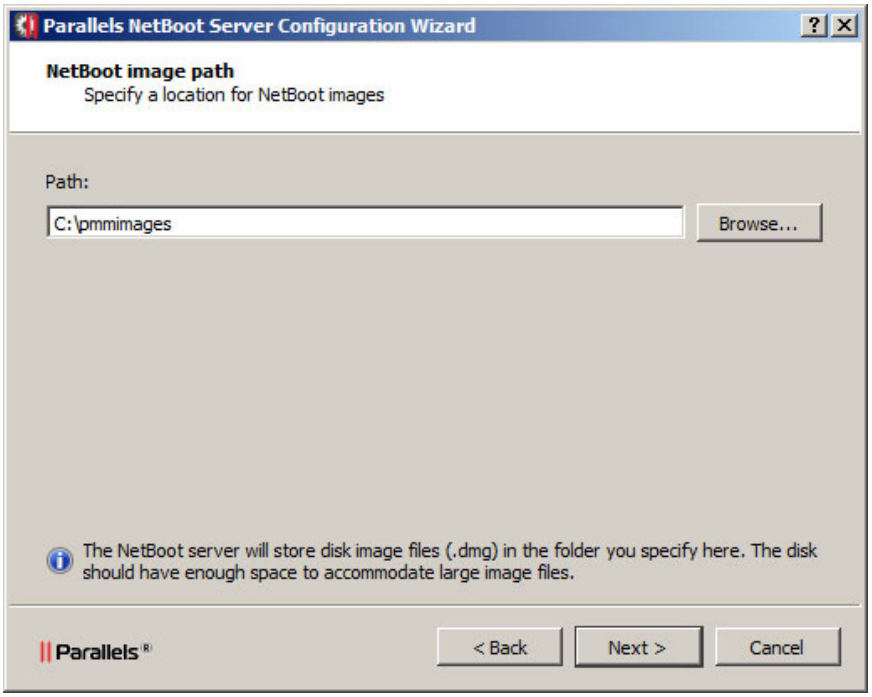
This account

Specifies a user account name. This can be a local or a domain user account. Enter the account name into the text field provided.

- **Browse** button — opens the standard Windows user account selection dialog where you can select an account from the list.
- **Password** — specifies the account password.

NetBoot Image Path Page

The **NetBoot image path** page is used to specify a folder where the NetBoot server will store `.dmg` images.

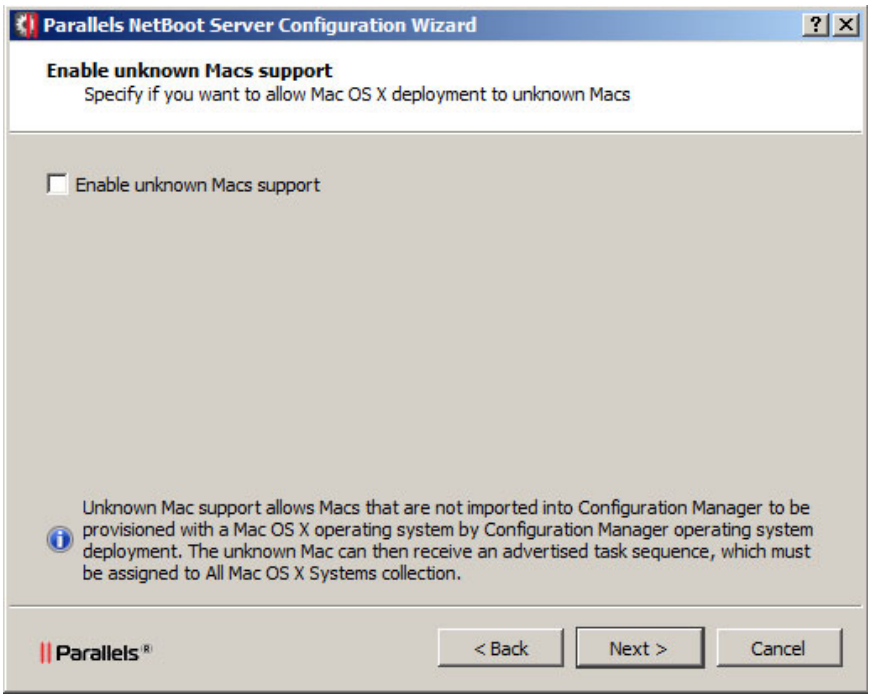

Parallels NetBoot Server Configuration Wizard
NetBoot image path
Specify a location for NetBoot images
Path:
C:\pmmimages
Browse...
The NetBoot server will store disk image files (.dmg) in the folder you specify here. The disk should have enough space to accommodate large image files.
Parallels
< Back
Next >
Cancel

The page contains the following elements:

Path
Specifies the image path.

Enable Unknown Macs Support Page

The **Enable unknown macs support** page allows you to specify whether the NetBoot server is allowed to work with Macs not assigned to the SCCM site. A Mac assigned to the site can be fully managed via SCCM. An unknown Mac is recognized on the network, but has not joined the SCCM site and therefore cannot be managed. You can enable the NetBoot server functionality for unknown Macs, so you can deploy Mac OS X images on them. Select the **Enable unknown Macs support** option to enable this feature. If the option is not selected, the NetBoot server will work only with Macs assigned to the site.


Parallels NetBoot Server Configuration Wizard
Enable unknown Macs support
Specify if you want to allow Mac OS X deployment to unknown Macs
Enable unknown Macs support
Unknown Mac support allows Macs that are not imported into Configuration Manager to be provisioned with a Mac OS X operating system by Configuration Manager operating system deployment. The unknown Mac can then receive an advertised task sequence, which must be assigned to All Mac OS X Systems collection.
Parallels
< Back
Next >
Cancel

The page contains the following elements:

Enable unknown Macs support
Select this option to enable support of unknown Macs. Clear the option to disable it.

Configuration Settings Summary Page

The **Configuration settings summary** page displays the NetBoot Server service configuration summary. Review the settings and click **Finish** to apply them or click **Back** to return to the previous page.

Configuration Progress Page

The **Configuration Progress page** displays the progress of the NetBoot server configuration procedure. The list displays the operations completed and the operations currently in progress.

Software Distribution Wizards

Create Package and Program Wizard

The **Create Package and Program Wizard** is used to create a software distribution package and a program. Please note that some options that can be set using the wizard are not used and will be ignored. The following describes which options are supported and which are not.

General page

Option	Supported	Description
Name	Yes	Package name.
Description	Yes	Package description.
Version	Yes	Package version.
This package contains source files	Yes	Check this option to add source files to the package.
Manufacturer	No	This field is ignored.
Language	No	This field is ignored.

Program Type page

All available options are supported.

Standard Program page

Option	Supported	Description
Name	Yes	Program name.
Command line	Yes	Specifies the command line.
Startup folder	No	This field is ignored.
Run	No	This field is ignored.
Program can run	No	This field is ignored.
Run mode	Yes	Specifies the run mode.
Allow users to view and interact with....	Yes	Allows to specify whether the Mac user can interact with the program.
Drive mode	No	This field is ignored.
Reconnect to distribution point at log on	No	This field is ignored.

Requirements page

Option	Supported	Description
Estimated disk space	Yes	Specifies the required disk space.
Maximum allowed run time	Yes	Specifies the maximum allowed runtime for the program.

All other fields on the **Requirements** page are ignored.

The **Summary**, **Progress**, and **Completion** pages don't have user editable fields.

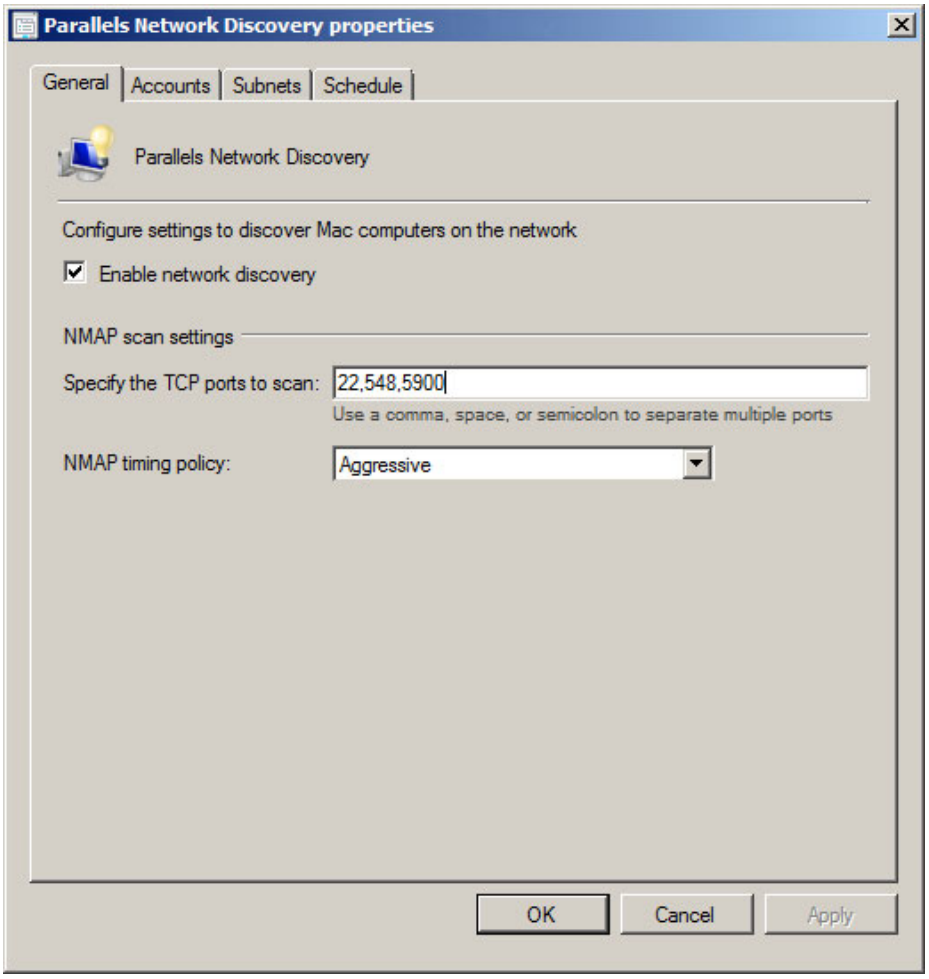
Property Pages

Parallels Discovery Properties

The **Parallels Discovery Properties** dialog displays information about discovery and provides controls to modify discovery properties. The discovery configuration is done through the individual tabs in this dialog.

Parallels Discovery Properties: General Tab

Use the **General** tab of the **Parallels Discovery Properties** dialog to enable or disable network discovery.



The **General** tab contains the following elements.

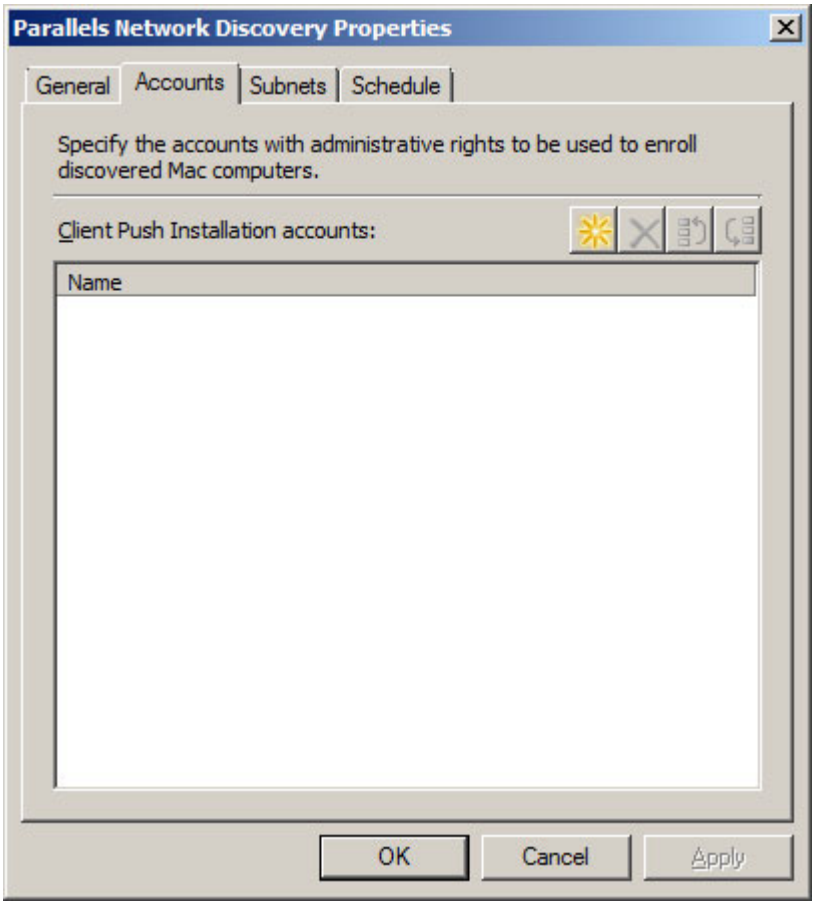
Enable network discovery
Enables or disables network discovery.

Nmap scan settings: Specify the TCP ports to scan
Specifies the ports to scan. You can enter multiple ports separated by a comma, space, or semicolon.

Nmap scan settings: Nmap timing policy
Specifies the Nmap timing policy.

Parallels Discovery Properties: Accounts Tab

Use the **Accounts** tab of the **Parallels Discovery Properties** dialog to specify the Mac OS X user information that will be used to log in to remote Macs. A user must exist on a Mac and must have administrative privileges. You can add more than one user to the list. The users will be used by discovery in the order listed.



The **Accounts** tab contains the following elements:

Client Push Installation Accounts list

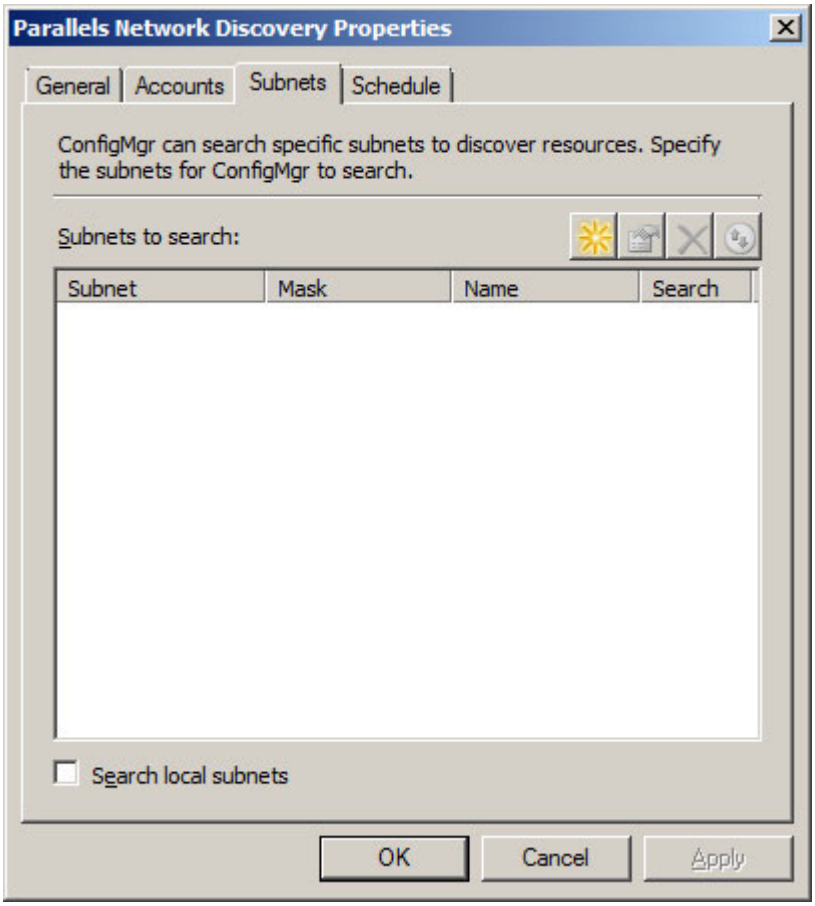
Contains the names of user accounts that discovery will use to log in to remote Mac computers.

The following options are available to manage user accounts:

- New icon: Opens the **Mac OS X User** dialog to add a Mac account.
- Delete icon: Deletes the selected account from the list.
- Move Up icon: Moves the selected account up one position on the displayed user list.
- Move Down icon: Moves the selected account down one position on the displayed user list.

Parallels Discovery Properties: Subnets Tab

Use the **Subnets** tab of the **Parallels Discovery Properties** dialog to specify the subnets to search during discovery.



The **Subnets** tab contains the following elements:

Subnets to search

Specifies the subnets that you want to search during Network Discovery.

The following options are available for managing the subnets searched during a Network Discovery run:

- New icon: Opens the **New Subnet Properties** dialog to add subnet information to the discovery polling list and to initially enable the specific subnet search.

  Note: Specifying a subnet does not guarantee that it will be searched, as this is influenced by the number of router hops selected.

- Property icon: Opens the **Subnet Properties** dialog to view or modify subnet information for a specific subnet from the discovery polling list.
- Delete icon: Removes the selected subnet from the discovery polling list.
- Enable/Disable icon: Enables or disables the selected subnet for discovery.

The following columns are displayed for each subnet in the discovery polling list:

- **Subnet**: Specifies a subnet number in IP format (for example: 131.24.10.0). This number can contain wildcards.
- **Mask**: Specifies the subnet mask for the subnet number (for example, 255.255.255.0).
- **Name**: Specifies the subnet name.
- **Search**: Specifies whether the subnet will be searched the next time discovery runs. Available options are **Enabled** and **Disabled**.

Search local subnets

Specifies whether subnets containing the server running discovery will be searched. This option is disabled by default.

Parallels Network Discovery: Boundaries Tab

Use the **Boundaries** tab page to specify Configuration Manager boundaries to search during network discovery. You can use this search option together with the options on the **Subnets** tab page, or you can use either one. If you haven't configured boundaries and boundary groups yet, you need to configure them before using this option (p. 36).

The **Boundaries** tab page has the following elements:

Boundary Groups to search list

Lists boundary groups. The groups displayed here are the groups that are used for the current site assignment (the **Use this boundary group for site assignment** option is selected in the boundary group **Properties** dialog). The groups that are not associated with any site are included in the list too. Highlight the group to display individual boundaries in the list below it. To search all boundaries in the group, select the check-box in front of the group name.

Boundaries to search list

Lists boundaries that belong to the highlighted boundary group. Select the boundaries to search.

Quick filter

Allows to specify a filter for the **Boundaries to search** lists. You can type any part of the text that might appear in the boundary's name, type, or description.

Check All

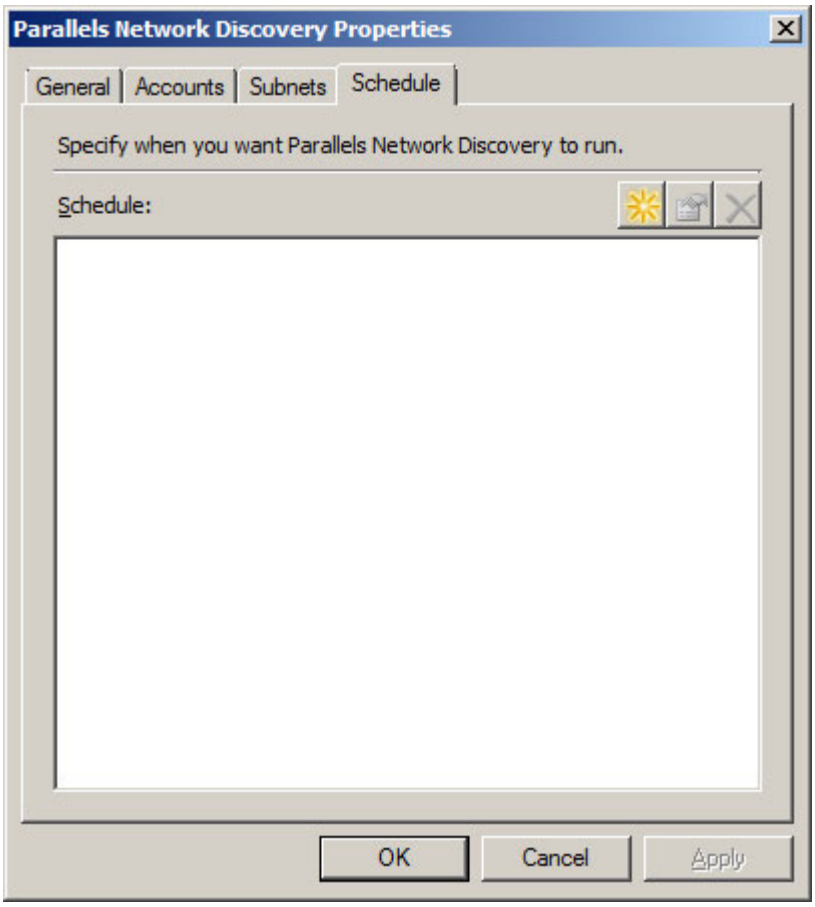
Selects all boundaries in the list.

Uncheck All

Clears all boundaries in the list.

Parallels Discovery Properties: Schedule Tab

Use the **Schedule** tab of the **Parallels Discovery Properties** dialog to set the Network Discovery schedule. Each schedule runs Network Discovery as currently configured. Although you can have multiple schedules, it is not possible to assign different configurations of Network Discovery to different schedules.



The **Schedule** tab contains the following elements:

Schedule

Specifies the schedules currently set to run Network Discovery.

The following options are available to manage Network Discovery schedules:

- New icon: Opens the **Custom Schedule** dialog to add a new schedule to the schedule list. This schedule may be for a one-time only run, or be a recurring schedule.
- Properties icon: Opens the **Custom Schedule** dialog to modify a selected schedule from the schedule list as needed.
- Delete icon: Deletes the selected schedule from the schedule list.

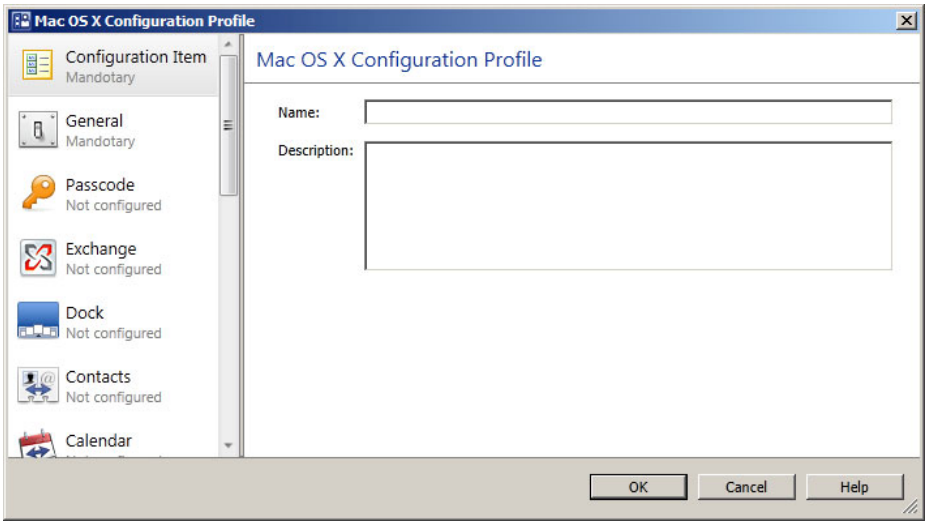
Dialog Pages

Desired Configuration Management Dialogs

The Desired Configuration Management dialogs are used to specify various configuration profiles on Macs that should be monitored for compliance.

Mac OS X Configuration Profile Dialog

Use this dialog to create a Mac OS X configuration profile. Mac computers will be evaluated for compliance using the configuration settings that you specify here.



The dialog contains the following elements:

Payload list (left pane)
Lists the available payloads.

Payload detail (right pane)
Contains elements representing the configurable options for the selected payload.

OK button

Saves the configuration item.

Cancel

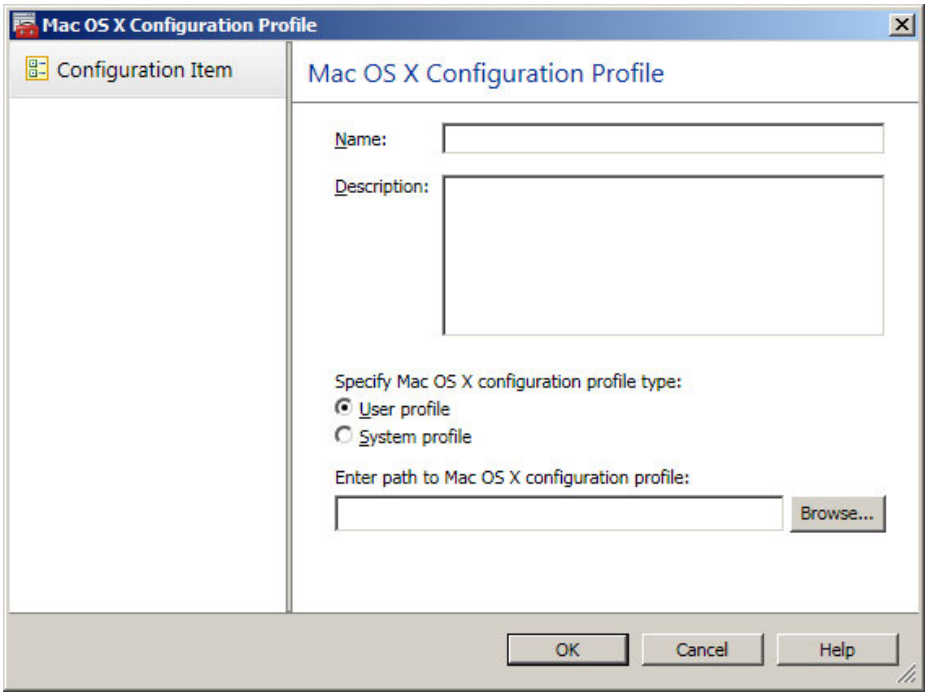
Closes the dialog without saving the configuration item.

Help

Displays this help topic.

Mac OS X Configuration Profile (from file) Dialog

Use this dialog to create a Mac OS X configuration item from an existing Mac OS X Configuration Profile file. Mac computers will be evaluated for compliance using the configuration contained in the specified file.



The dialog contains the following elements:

Name

User-defined configuration item name.

Description

User-defined configuration item description (optional).

User profile

Select this option if you want to install the configuration profile using the current user's security context. Note that the System Policy Control payload (designated by specifying `com.apple.systempolicy.control` as the PayloadType) must only exist in a device profile. If the payload is present in a user profile, an error will be generated during installation and the profile will fail to install.

System profile

Use this option when you want to install the configuration profile as `root`.

Enter path to Mac OS X configuration profile

Specifies the path to the Mac OS X Configuration Profile file (the file with the ".mobileconfig" extension).

Browse button

Click the **Browse** button to locate and select the Mac OS X configuration profile (the file with the ".mobileconfig" extension).

OK button

Saves the configuration item.

Cancel

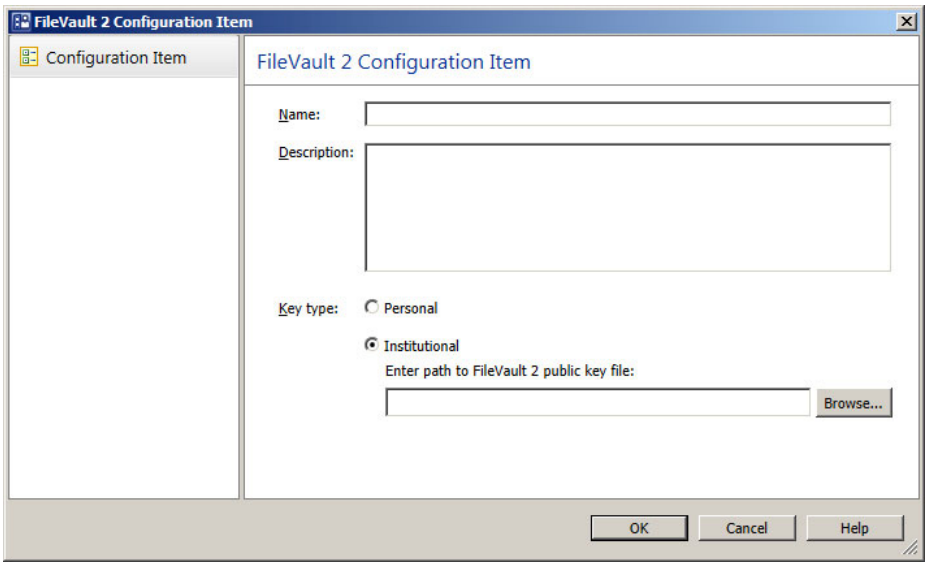
Closes the dialog without saving the configuration item.

Help

Displays this help topic.

FileVault 2 Configuration Item Dialog

Use this dialog to create a configuration item containing Mac OS X FileVault 2 settings.



The dialog contains the following elements:

Name
Specifies the configuration item name.

Description
Specifies the configuration item description.

Key type: Personal
If this option is selected, a personal key will be used to encrypt each Mac.

Key type: Institutional
If this option is selected, an institutional key will be used to encrypt all Macs to which this configuration item will be applied.

Browse
The button is enabled when the Key type: Institutional option is selected. The button opens a window where you can browse for the `FileVaultMaster.keychain` file. See Creating FileVault 2 Configuration Item for the instructions on how to create the file.

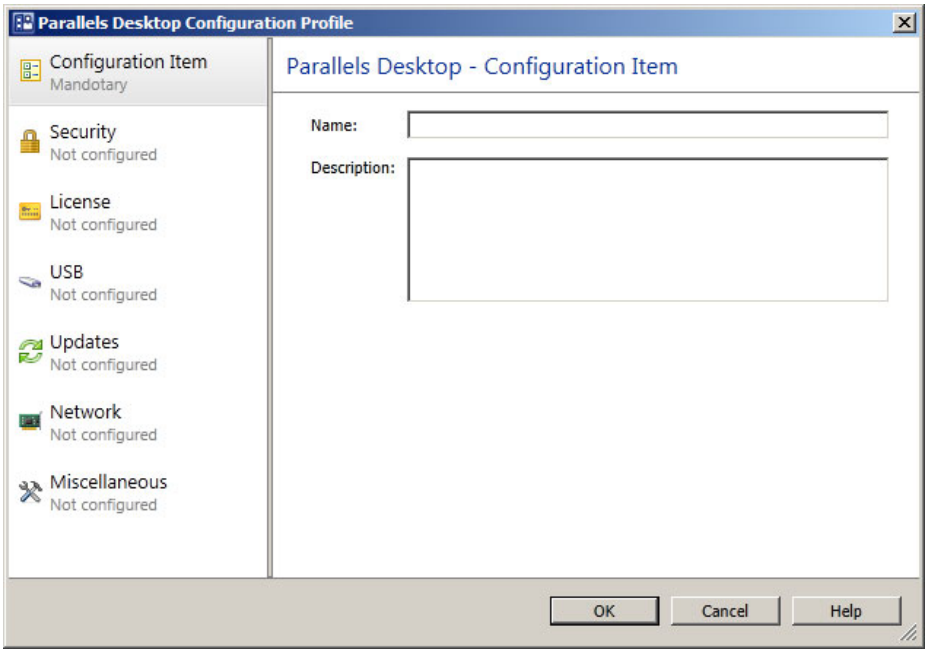
OK
Saves the configuration item and closes the dialog.

Cancel
Cancels the changes and closes the dialog..

Help
Opens this help page.

Parallels Desktop Configuration Profile Dialog

Use this dialog to create a Parallels Desktop configuration profile. Parallels Desktop on Mac computers will be evaluated for compliance using the configuration that you specify here.



The configuration options in the dialog are grouped by functionality. To make modifications:

1. Select an item in the left pane.
2. The right pane is populated with the corresponding configuration options.
3. Toggle the ON/OFF switch of an option you want to modify by clicking it and set the desired value.

   Note: Options with the ON/OFF switch set to "OFF" will not be evaluated on a client Macs.

4. Click the **OK** button to save the configuration item. Click **Cancel** to cancel the changes.

The elements in the dialog mimic the **Parallels Desktop Preferences** window on a Mac. For more information on how to modify Parallels Desktop preferences, please refer to **Parallels Desktop User's Guide**. For information about the configuration options specific to Parallels Desktop Enterprise Edition, see the **Parallels Desktop Mass Deployment Guide.**

The dialog contains the following elements:

Configuration Item
Specifies the configuration item name and description.

Security
Specifies Parallels Desktop security settings.

License
Specifies Parallels Desktop license information.

USB
Specifies USB settings.

Updates
Specifies Parallels Desktop automatic update options.

Network
Specify networking settings.

Miscellaneous
Specifies miscellaneous configuration options.

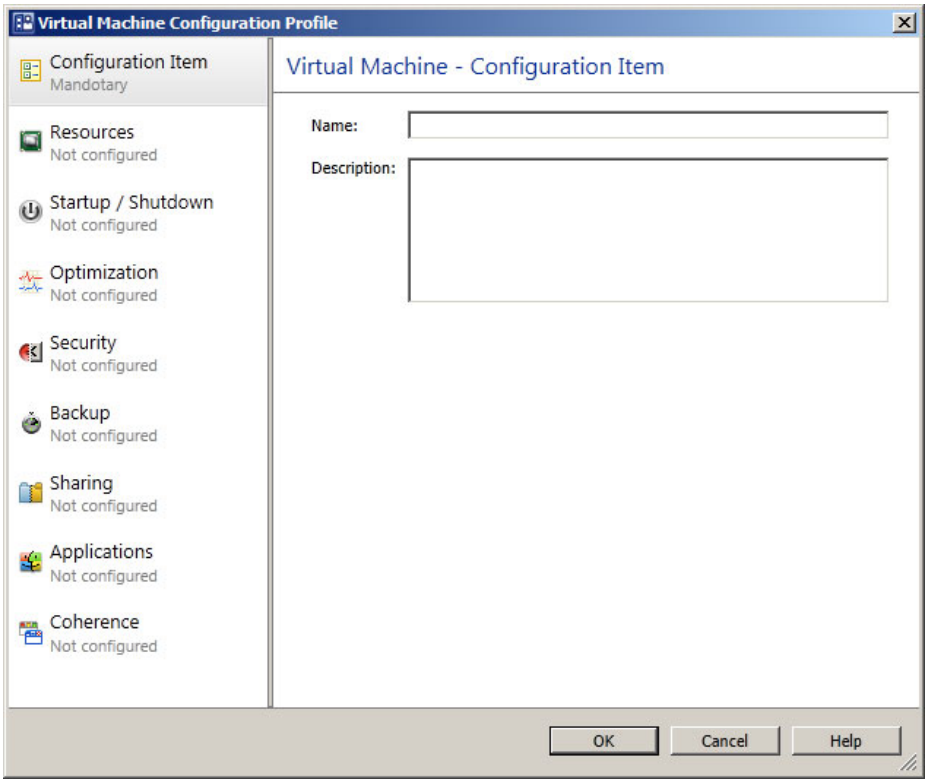
OK button
Saves the configuration item.

Cancel button
Cancels the changes and closes the dialog.

Help button
Opens this help topic.

Virtual Machine Configuration Profile Dialog

Use this dialog to create a configuration item containing Parallels virtual machine configuration settings. Virtual machines on client Macs will be evaluated against the configuration settings that you specify here.



The configurations options in the dialog are grouped by functionality. To make modifications:

1. Select an item in the left pane.
2. The right pane is populated with the corresponding configuration options.
3. Toggle the ON/OFF switch of an option you want to modify by clicking it and set the desired value.

   Note: Options with the ON/OFF switch set to "OFF" will not be evaluated on a client Macs.

4. Click the **OK** button to save the configuration item. Click **Cancel** to cancel the changes.

The elements in this dialog mimic the elements in the **Virtual Machine Configuration Options** window on a Mac. For more information on how to modify a virtual machine configuration, please refer to **Parallels Desktop User's Guide**.

The dialog contains the following elements:

Configuration Item

Specifies the configuration item name and description.

Resources
Specifies the CPU, RAM, video memory, and boot settings.

Startup / Shutdown
Specifies virtual machine startup and shutdown settings.

Optimization
Specifies performance, power, and free space optimization settings.

Security
Specifies virtual machine security settings, including password-protecting virtual machine actions and blocking the Mac user from modifying a virtual machine configuration.

Backup
Specifies virtual machine backup settings.

Sharing
Specifies Mac OS X and Windows folder sharing settings.

Applications
Specifies Windows and Mac application sharing settings.

Coherence
Specifies Coherence settings.

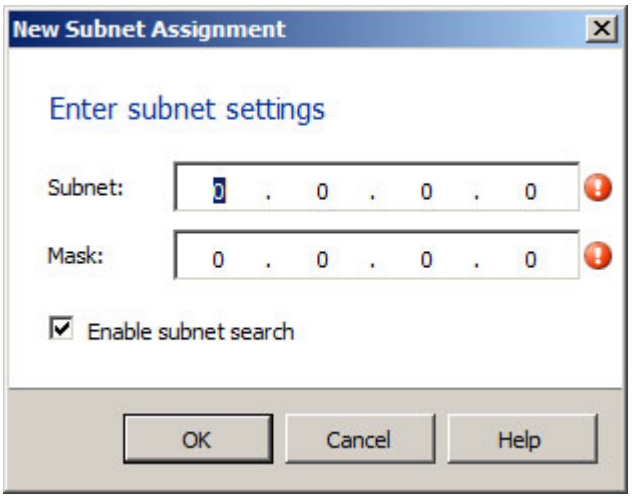
OK button
Saves the configuration item.

Cancel button
Cancels the changes and closes the dialog.

Help button
Opens this help topic.

New Subnet Assignment Dialog

Use this dialog to specify a subnet to be searched by Network Discovery.



The dialog contains the following elements:

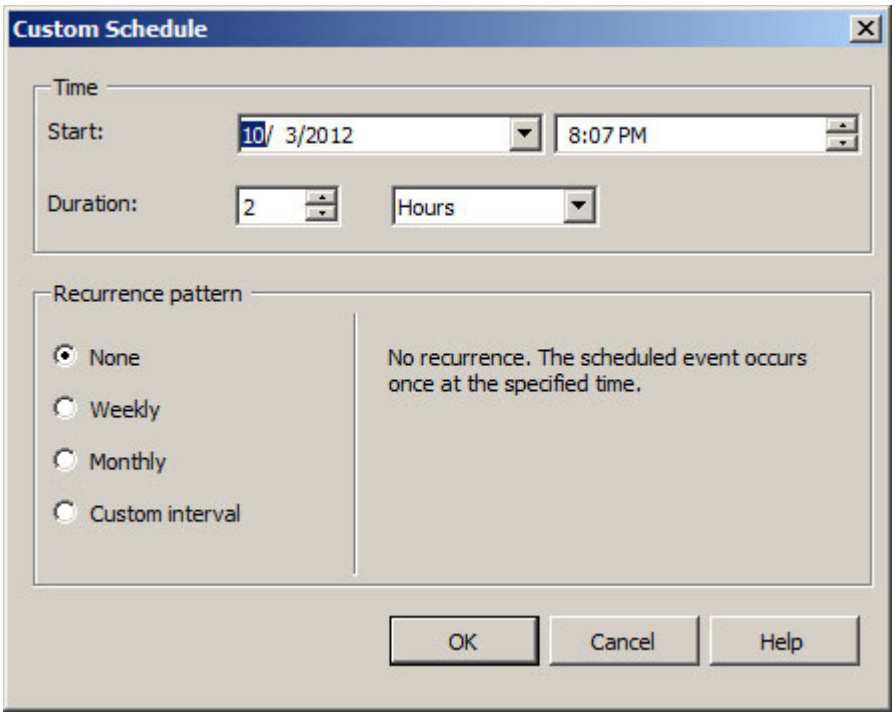
Subnet
A subnet number in IP format (for example, 131.24.10.0) to be searched by Network Discovery.

Mask
The subnet mask for the subnet number (for example, 255.255.255.0).

Enable subnet search
Enables Network Discovery in the specified subnet. This subnet's status (enabled or disabled) is shown in the Search column in the Subnets tab of the Network Discovery dialog.

Custom Schedule Dialog

Use this dialog to schedule the start, recurrence pattern, and duration of an operation.



The dialog contains the following elements:

Time

Specifies the Start date and time or Duration of the operation.

Recurrence Pattern

Specifies how often this operation recurs.

The following options are available for setting a recurrence pattern:

- None: Specifies that the operation does not recur.
- Weekly: Specifies that the operation recurs every N weeks. If this option is selected, you must specify the day of the week on which the operation will occur.
- Monthly: Specifies that the operation recurs every N months. If this option is selected, you must specify the day of the month on which the operation will occur.
- Custom interval: Specifies the frequency with which the operation will recur. You may set this in terms of minutes, hours, or days, with the following available values:

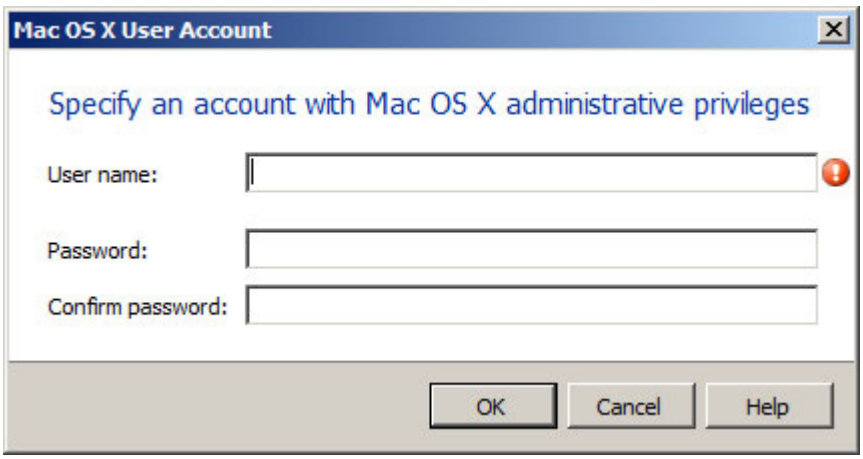
  Minutes: Values from 1 to 59 minutes, inclusive.

  Hours: Values from 1 to 23 hours, inclusive.

Days: Values from 1 to 31 days, inclusive.

Max OS X User Account Dialog

Use this dialog to specify a Mac OS X user account that Network Discovery should use to connect to remote Mac computers. The user account must have administrative rights on the Mac.



The dialog contains the following elements:

User Name
Specifies the Mac OS X user account name.

Password
Specifies the Mac OS X user account password.

Confirm Password
Specifies the Mac OS X user account password for confirmation.

Problem Report for Parallels Mac Management for Microsoft SCCM Dialog

Use this dialog to send a problem report to Parallels Support when you are having a problem with the Parallels Mac Management for Microsoft SCCM. The dialog will collect system data for the Parallels Mac Management components and for the selected Mac computer and will forward this information to the Parallels Support server.

The dialog contains the following elements:

Please describe what you were doing when the problem occurred?
Use this edit box to describe the problem in your own words.

Send Report button

Click the **Send Report** button to collect the report data and send it to Parallels Support. A progress bar will be displayed informing you of the data collection progress.

Close button

Click the **Close** button to close the dialog.

Send Problem Report Dialog

Use this dialog to send a problem report to Parallels Support.

The dialog contains the following elements:

Report file location:

The name and path of the file containing the report. This is a temporary location. The file will be deleted from it after the report is sent to Parallels Support or the dialog is closed.

Send button

Click the **Send** button to send the report to Parallels Support. After the report is sent, a message box containing the problem report number is displayed. You can use this number for future reference. The problem report file is automatically deleted from the temporary location specified in the **Report file location** text box.

Cancel button

Click the **Cancel** button to close the dialog. The problem report file will be deleted from the location specified in the **Report file location** text box. If the utility is run on the computer where the Configuration Manager Proxy is installed, the report will be forwarded to Configuration Manager Proxy, which will notify the Problem Monitor about it. You can then use the Problem Monitor to send the report to Parallels Support or you can permanently delete it. For more info, see **Using Problem Monitoring Utility**.

Problem Reports Dialog

Use this dialog to view the available Parallels Mac Management problem reports.

The dialog contains the following elements:

Problem report list

Lists the available reports. Each row contains the information about an individual report and has the following columns:

- **Created** — contains the date and time when the report was created.
- **Proxy info** — if set to "Yes", indicates that the report contains the information related to the Configuration Manager Proxy.
- **Mac info** — if set to "Yes", indicates the the report contains the information related to a managed Mac computer.

- **Description** — specifies whether the report was generated automatically or manually by a user.

Send Report button

Sends the selected problem report to Parallels Support and removes the report from the list. The report is also deleted from the server on which it resides.

Delete button

Removes the reports from the list and from the server on which it resides.

Close button

Closes the dialog.

CHAPTER 7

Appendices

In This Chapter

Ports Used by Parallels Mac Management 147
Log Files in Parallels Mac Management for Microsoft SCCM 148
Changing Log File Rotation Limits 151
Parallels Mac Management Database..... 153

Ports Used by Parallels Mac Management

The following table describes the ports used by Parallels Mac Management for Microsoft SCCM. The list does not include the ports used by the standard System Center Configuration Manager 2012 services and by the standard Windows services.

Program	TCP	UDP	Platform	Required	Notes
Configuration Manager Proxy pma_isv_proxy_service.exe	8760, 8761		Windows	Required	The default ports 8760 and 8761 can be changed if needed using the Configuration Manager Proxy configuration utility.
NetBoot Server pma_netboot_service.exe bootpd (DHCP)		67, 68	Windows	Optional	Required for the NetBoot Server functionality.
NetBoot Server pma_netboot_service.exe tftpd (TFTP)		69	Windows	Optional	Required for the NetBoot Server functionality.
NetBoot Server pma_netboot_service.exe HTTPD (Web)	80		Windows	Optional	Required for the NetBoot Server functionality.
SSH server	22		Mac	Optional	Required for the Network Discovery functionality.
VNC server	5900		Mac	Optional	Needed to accept VNC connections on a Mac.

Mac client	8000		Mac	Required	Required for Parallels Mac Client to accept incoming connection from Parallels Configuration Manager Proxy.

In addition, RPC ports need to be open in order to allow WMI/RPC traffic to pass through. RPC ports can be opened by enabling a Group Policy firewall exception. Open the Group Policy Object Editor snap-in (gpedit.msc) to edit the Group Policy object (GPO) that is used to manage Windows Firewall settings in your organization. Open **Computer Configuration**, open **Administrative Templates**, open **Network**, open **Network Connections**, open **Windows Firewall**, and then open either **Domain Profile** or **Standard Profile**, depending on which profile you want to configure. Enable the following exception: "Allow Remote Administration Exception".

Log Files in Parallels Mac Management for Microsoft SCCM

Parallels Mac Management maintains its own log files which capture information about its processes. The log files are created and maintained for each component including Configuration Manager Proxy, Configuration Manager Console Extension, and clients running on individual Mac computers. Some information about Parallels Mac Management processes is also recorded in the System Center Configuration Manager log files. You can use the information contained in the log files to help you troubleshoot issues that might occur in the Parallels Mac Management for Microsoft SCCM.

Parallels Mac Management for Microsoft SCCM Log Files

The Parallels Mac Management log files are located in the following directories:

- Windows computer running Configuration Manager Proxy: `%Windir%\Logs`
- Windows computer running Configuration Manager console: `%Windir%\Logs`
- Mac OS X (client software): `/Library/Logs/`

The following table describes the Parallels Mac Management for Microsoft SCCM log files:

Component	Log File Name	Log File Description
SCCM Proxy	pma_setup.log	This log file is created during the SCCM Proxy installation. It contains information about the installation procedures and the changes they make to the system. Please note that when the SCCM Proxy and the SCCM Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
	pma_isv_proxy_config.log	This log file is created and updated every time the SCCM Proxy configuration utility is run. It contains information about the configuration parameters selected by the user (SMS Provider, service account name, etc.) and the results of the configuration operations.

	pma_isv_proxy_service.log	This is the main SCCM Proxy log file. It is updated as needed while the SCCM Proxy service is running. It contains information related to the SCCM Proxy operations such as starting/stopping the service, reading various system properties, starting or stopping Mac management utilities and others.
	pma_discovery.log	This log file is updated every time a network discovery (manual or scheduled) is run. It contains information about the discovery itself (processes started, subnets searched, etc) and the information about discovered Mac computers, including IP address, hostname, MAC address, whether the Client installation was initiated on a Mac, and other info.
SCCM Console Extension	pma_setup.log	The SCCM Console Extension component has just one log file: pma_setup.log. The file contains information about the component installation procedure. Please note that when the SCCM Proxy and the SCCM Console Extension components are installed on the same computer, the pma_setup.log is shared between them.
Mac Client	pma_agent.log	This is the main client software log file, which contains information about the client operations. The file is updated when the Mac Client communicates with SCCM Proxy and/or performs actions on the Mac computer on which it is running.
	pma_agent_ui.log	This log file is updated when the client installation and registration utilities are run on the Mac by a user. The file also records information when an operation is performed on the Mac that is user-specific. An example of such an operation is applying a Mac configuration profile (a profile is applied for each individual Mac user if more than one user exists). Please note that if a Mac user doesn't have privileges to write to the /Library/Logs directory, the log file will be created in the /Users/<*user_name*>/Library/Logs directory.
	pma_agent_uninstaller.log	This log file is created when the client is uninstalled from the Mac computer.

System Center Configuration Manager Log Files

Some of the Parallels Mac Management process information is recorded in the SCCM log files. You may examine these files in addition to the log files described above. Please note that SCCM creates these files on the fly and not all of them may actually exist.

The following table describes the Site Server log files which are located in the `<SCCM_InstallationPath>\LOGS` folder. The files may contain information about the SCCM Proxy component.

Log file	Log file description
Colleval.log	Records activities when collections are created, changed, and deleted by the Collection Evaluator.
Dataldr.log	Processes Management Information Format (MIF) files and hardware inventory in the Configuration Manager database.
Ddm.log	Saves DDR information to the Configuration Manager database by the Discovery Data Manager.
Distmgr.log	Records package cration, compression, delta replication, and information updates.
Offermgr.log	Records advertisement updates.
Offersum.log	Records summarization of advertisement status messages.
Policypv.log	Records updates to the client policies to reflect changes to client settings or advertisements.
Smsprov.log	Records WMI provider access to the site database.
statesys.log	Records the processing of state system messages.

The following table describes the Management Point log files, which are located in the `%ProgramFiles%\SMS_CCM\Logs` folder. The files may contain information about the SCCM Proxy component.

Log file	Log file description
MP_CliReg.log	Records the client registration activity processed byt the management point.
MP_Ddr.log	Records the conversion of XML.ddr records from clients, and copies them to the site server.
MP_Framework.log	Records the activities of the core management point and client framework components.
MP_GetAuth.log	Records the status of the site management points.
MP_GetPolicy.log	Records policy information.
MP_Hinv.log	Converts XML hardware inventory records from clients and copies the files to the site server.
MP_Location.log	Records location manager tasks.
MP_OOBMgr.log	Records the management point activities related to receiving OTP form a client (SCCM 2012 only).
MP_Policy.log	Records policy communication.
MP_Relay.log	Copies files that are collected from the client.
MP_Retry.log	Records the hardware inventory retry processes.
MP_Sinv.log	Converts XML software inventory records from clients and copies them to the site server.
MP_SinvCollFile.log	Records details about file collection (SCCM 2012 only).

MP_Status.log	Converts XML.svf status message files from clients and copies them to the site server.

The following table describes the Admin UI log files, which are located in the `<SCCM_InstallationPath>\AdminUI\AdminUILog` directory. The files may contain information about the Configuration Manager Console Extension component.

Log file	Log file description
ResourceExplorer.log	Records errors, warnings, and information about running the Resource Explorer.
SMSAdminUI.log	Records the local Configuration Manager console tasks when you connect to the Configuration Manager site.

Parallels Mac Management for Microsoft SCCM Crash Dumps

In addition to log files, crash dumps may be generated if a Parallels Mac Management component terminates abnormally. The crash dumps are generated for the Configuration Manager Proxy component and for Mac Clients running on individual Macs. Please note that crash dumps may not be created every time a component crashes. If a dump doesn't exist in the directories specified below, it can be found in the problem report, which will be generated instead.

The crash dump file locations are:

- Configuration Manager Proxy: `%ALLUSERSPROFILE%\Microsoft\Windows\WER\ReportQueue\AppCrash_pma_isv_proxy_*`, where `AppCrash_pma_isv_proxy_*` is the name of a directory containing the crash dump files (the name is appended with a unique suffix for each dump).
- Mac client software: `/Library/Logs/CrashReporter/pma_agent*.crash`, where `pma_agent*.crash` is the name of the directory containing the files (the asterisk character is substituted with a unique dump identifier).

Changing Log File Rotation Limits

About Log File Rotation

Parallels Mac Management for Microsoft SCCM 2012 implements log file rotation that ensures that the log files don't grow in size indefinitely. The amount of data contained in an individual log file and the total size of all logs are kept at a reasonable limit. Log file rotation is enabled by default.

Parallels Mac Management for Microsoft SCCM 2012 consists of a number of executables including services, graphical user interface, and utilities. Each executable creates its own log file named <exec_name.log>, where "exec_name" is the executable file name. The following table lists Parallels Mac Management executables and their corresponding log file names and locations:

Executable Name	Operating System	Log File Name and Path
pma_isv_proxy_service	Windows	%Windir%\Logs\pma_isv_proxy_service.log
pma_isv_proxy_config	Windows	%Windir%\Logs\pma_isv_proxy_config.log

pma_discovery	Windows	%Windir%\Logs\pma_discovery.log
pma_problem_monitor	Windows	%Windir%\Logs\pma_problem_monitor.log
pma_report_tool	Windows Mac OS X	%Windir%\Logs\pma_report_tool.log /Users/<user_name>/Library/Logs
pma_agent	Mac OS X	/Library/Logs/pma_agent.log
pma_agent_ui	Mac OS X	/Library/Logs/pma_agent_ui.log

A log file is populated with data when an executable is running and performing its tasks. When the size of a log file exceeds a predefined limit, the file is archived and a new empty log file is created in its place. This creates a log file rotation set consisting of the current log file and archived files. A log file rotation set is managed using the following rules:

- Log files are archived using the zlib compression library.
- The archived files in the set are named as follows:

  `<exec_name.1.log.gz>`, `<exec_name.2.log.gz>`, `<exec_name.3.log.gz>`, etc.

  The `<exec_name.1.log.gz>` file is the most recently archived log segment. The file with the largest sequential number in its name is the oldest. When the current log file is archived, it is named `<exec_name.1.log.gz>`. The existing archives are renamed by incrementing the sequential number in their names by 1. The maximum number of files in a rotation set can be configured (see **Changing Log File Rotation Limits** below). When the number of files exceeds the predefined limit, the oldest file is deleted.
- Rotation of each log is performed independently from other logs.

Changing Log File Rotation Limits

Log file rotation limits are configured similarly on both Windows and Mac OS X computers. The following rules apply when specifying the limits:

- **Log file size limit**. The default value is 1 MB (specified in bytes). The minimum allowed value is 200 KB. The maximum allowed value is 4 MB. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.
- **Maximum number of files in a rotation set**. The default value is 10. The minimum value is 1. The maximum value is 20. If a value is not set, the default value is used. If the specified value falls outside the min/max interval, the minimum or the maximum value is used respectively.

On Windows computers the log rotation limits are stored in the system registry. To modify the limits:

- Run "regedit" and search for HKEY_LOCAL_MACHINE\SOFTWARE\Parallels\Parallels Management Suite for Microsoft SCCM\Preferences.
- To set the log file size limit, modify the value of the "LogFileSizeLimit" parameter. The size is specified in bytes.

- To set the maximum number of files in a rotation set, modify the value of the “MaxNumberOfSavedLogs” parameter.

On Mac OS X computers, the log rotation limits are stored in the `/Library/Preferences/com.parallels.pma.agent.plist` file. To modify the limits:

- Open the `com.parallels.pma.agent.plist` file in a text editor.
- To set the log file size limit, modify the value of the "LogFileSizeLimit" parameter. The size is specified in bytes.
- To set the maximum number of files in a rotation set, modify the value of the “MaxNumberOfSavedLogs” parameter.

Parallels Mac Management Database

When Parallels Mac Management for Microsoft SCCM is installed, it creates its own SQL Server database on the primary SCCM site to store security data such as recovery keys, certificates, and other.

The database name is constructed using the following syntax:

`PMM_`<*site_name*>

Where, `PMM_` is used as-is and <*site_name*> is the name of the primary SCCM site.

At the time of this writing, the database is used to store the FileVault 2 disk encryption information and recovery keys. Other security related data may be stored in the database in the future.

The system administrator should backup the database regularly in order to ensure the data safety.

Index

A

About Parallels Mac Management for Microsoft SCCM 2012 - 7
About This Guide - 7
Appendices - 148
Application Management - 89

C

Certificate Authority and PKI Integration Overview - 20
Changing Log File Rotation Limits - 152
Checking Installation Requirements - 10
Checking User Rights Requirements - 14
Choosing Installation Type - 89
Configuration Manager Proxy Communication Ports Page - 124
Configuration Manager Proxy Service Account Page - 120
Configuration Progress Page - 128
Configuration Settings Summary Page - 124, 128
Configuring Certificate Authorities and PKI Integration - 20
Configuring Configuration Manager Boundaries - 36
Configuring Deployment Type - 92
Configuring Inventory Settings - 58
Configuring Mac OS X Firewall - 47
Configuring Windows Firewall - 37
Create Package and Program Wizard - 129
Creating Certificate Templates for Parallels Proxy and Macs - 29
Creating Compliance Rules - 86
Creating Configuration Item - 83
Creating Configuration Manager Application - 91
Creating Custom Workstation Authentication Certificate Template - 25
Creating Discovery Script - 85
Creating FileVault 2 Configuration Item - 68, 75
Creating FileVaultMaster Keychain - 68
Creating OS X Configuration Profile - 60
Creating OS X Configuration Profile from File - 64
Creating Remediation Script - 85
Creating Software Distribution Package - 98
Creating Special Security Group - 30
Custom Schedule Dialog - 144

D

Deploying Certificate to Web Server - 22
Deploying Client Certificate to Distribution Point - 24
Deploying Configuration Baseline - 87
Deploying Mac Application - 94
Deploying Mac Client via Network Discovery - 41
Deploying Mac OS X Images - 102
Deploying OS X Configuration Profile - 60
Deploying Parallels Desktop and Virtual Machines on Macs - 106
Deploying Parallels Mac Client - 41
Deploying Parallels Mac Management for Microsoft SCCM 2012 - 9
Deploying PKI Certificates - 21
Deploying SCCM Client in Windows Running in a Virtual Machine - 109
Deploying Software - 101
Desired Configuration Management - 59
Desired Configuration Management Dialogs - 135
Dialog Pages - 135

E

Enable Unknown Macs Support Page - 128
Enforcing FileVault 2 Encryption - 67
Enforcing Parallels Desktop Preferences - 80
Enforcing Parallels Desktop VM Settings - 82

Exporting Client Certificate for Distribution Point - 26

F

FileVault 2 Configuration Item Dialog - 137
FileVault 2 Encryption with Institutional Recovery Key - 68
FileVault 2 Encryption with Personal Recovery Key - 74

H

Hardware and Software Inventory - 58

I

Initiating Policy Retrieval - 53
Installing Active Directory Certificate Services Role - 21
Installing Application on a Mac - 96
Installing Custom Workstation Authentication Certificate - 26
Installing Mac Client Using Installation Script - 46
Installing Mac Client Using Interactive Installer - 44
Installing Parallels Mac Management for Microsoft SCCM 2012 - 31
Introduction - 7

L

Log Files in Parallels Mac Management for Microsoft SCCM - 149

M

Mac OS X Configuration Profile (from file) Dialog - 136
Mac OS X Configuration Profile Dialog - 135
Management Point Location and SCCM Site Code Page - 121
Managing Parallels Mac Client - 51
Max OS X User Account Dialog - 145
Migrating Configuration Manager Proxy - 38

N

NetBoot Image Path Page - 127
New Subnet Assignment Dialog - 143

P

Parallels Configuration Manager Proxy Configuration Wizard - 32, 119
Parallels Desktop Configuration Profile Dialog - 139
Parallels Discovery Properties - 130
  Accounts Tab - 131
  General Tab - 130
  Schedule Tab - 134
  Subnets Tab - 132
Parallels Mac Management Component Overview - 9
Parallels Mac Management Database - 154
Parallels Mac Management Features - 57
Parallels Mac Management for Microsoft SCCM Setup Wizard - 31
Parallels NetBoot Server Configuration Wizard - 34, 125
Parallels NetBoot Server Service Account page - 125
Parallels Network Discovery Boundaries Tab - 133
Ports Used by Parallels Mac Management - 148
Preparing Mac Application for Configuration Manager - 90
Problem Report for Parallels Mac Management for Microsoft SCCM Dialog - 145
Problem Reporting and Monitoring - 112
Problem Reports Dialog - 146
Property Pages - 130
Providing Remote Assistance to Mac Users - 111

R

Receiving DCM Reports - 88
Recovering Encrypted Disk Using Institutional Key - 72
Recovering Encrypted Disk Using Password - 72, 78
Recovering Encrypted Disk Using Personal Key - 78

S

Security Settings Page - 122
Send Problem Report Dialog - 146

Sending Package to Distribution Point - 101
Sending Problem Reports from Mac Client - 114
Sending Problem Reports From Mac Client - 55
Sending Problem Reports Using Configuration Manager Console - 112
Sending Problem Reports Using Windows Reporting Utility - 113
SMS Provider Location Page - 120, 125
Software Distribution - 98
Software Distribution Wizards - 129
Specifying Script Interpreter - 86
Switching SCCM Roles from HTTP to HTTPS - 27

T

Technical Reference - 119
Tracking Apple Warranty Status of Macs - 117

U

Understanding Collections in Parallels Mac Management - 57
Uninstalling Parallels Mac Client - 49
Updating Parallels Configuration Manager Proxy Connection URL - 48
Upgrading Parallels Mac Client - 49
Upgrading Parallels Mac Management for Microsoft SCCM 2012 - 36
User Rights Required for Installing and Configuring Parallels Mac Management - 14
User Rights Required for Running Parallels Configuration Manager Proxy Service - 18
Using Configuration Manager 2012 Console - 57
Using Parallels Application Portal - 97
Using Problem Monitoring Utility - 115
Using Scripts to Assess Compliance - 83

V

Verifying Mac Client Deployment - 48
Viewing and Monitoring FileVault 2 Encryption Status - 70, 76
Viewing Inventory Data - 59
Viewing Parallels Mac Client Properties - 51
Viewing Proxy Service Certificate Details - 37
Viewing Status of a Package - 102
Virtual Machine Configuration Profile Dialog - 141

W

Wizard Pages - 119